

Instalación de telefonía Cisco e integración y configuración de Asterisk dentro de la estructura telefónica de Labco



**Proyecto Final de Carrera de Ingeniería en
Informática**

Autor: Gonzalo Calvo Ceinos

Director: Edgar Navarro Andrés

Ponente: René Serral Gracià

Fecha: Marzo 2012

AGRADECIMIENTOS

Este proyecto no se podría haber llevado a cabo sin la colaboración y ayuda de un gran número de personas.

En primer lugar quiero dar las gracias a mi director de proyecto Edgar Navarro, por darme la oportunidad de realizar el proyecto que necesitaba para la empresa. También agradecer a mi ponente René Serral por guiarme y aconsejarme durante todos estos meses.

Gracias también a todo el personal de Labco, en especial al departamento de sistemas, Alberto Martín, Marçal Montserrat, Javier Clarés, Josep Maria Ros y Daniel Ros por su apoyo y consejos durante todo el proyecto.

Gracias a toda mi familia y amigos por darme su apoyo durante toda la carrera.

No quiero acabar estas líneas sin agradecer a la persona que más me ha ayudado en los buenos y sobretodo en los malos momentos y que más me ha comprendido, gracias Ada.

ÍNDICE

1	INTRODUCCIÓN	9
1.1	Objetivos.....	10
1.2	Planificación	10
2	CONCEPTOS GENERALES	12
2.1	VoIP.....	12
2.1.1	¿Qué es VoIP?	12
2.1.1.1	Ventajas de VoIP	13
2.1.1.2	Desventajas de VoIP.....	13
2.1.2	Elementos necesarios en una red VoIP.....	14
2.1.3	Protocolos de VoIP	15
2.1.3.1	SIP	15
2.1.3.1.1	Comunicación SIP	17
2.1.3.2	SCCP	18
2.1.3.3	H.323	18
2.1.3.4	IAX.....	19
2.1.3.5	Otros protocolos	19
2.1.4	Parámetros VoIP.....	20
2.1.4.1	Códecs	20
2.1.4.2	QoS.....	20
2.1.5	VoIP en el modelo OSI.....	22
3	TELEFONÍA CISCO	23
3.1	La telefonía IP de Cisco.....	23
3.2	Tecnología utilizada en la telefonía IP	24
3.2.1	Centralitas.....	24
3.2.2	Teléfonos y terminales.....	25
3.3	Las comunicaciones.....	28
3.3.1	Punto de partida	28
3.3.2	Nuevas comunicaciones	28
3.3.3	Tecnología utilizada para la conexión.....	30

3.3.4	Interconexión de sedes.....	31
3.3.5	Seguridad en las conexiones.....	32
3.3.6	Topología de la red.....	33
3.4	Configuración básica de Cisco Unified Communications Manager	41
3.4.1	Introducción.....	41
3.4.2	Administración del sistema (System).....	42
3.4.2.1	Configuración de la IP del servidor.....	43
3.4.2.2	Configuración de la referencia NTP.....	45
3.4.2.3	Configuración de fecha y hora	46
3.4.2.4	Configuración del SRST.....	48
3.4.2.5	Configuración de las Device Pool.....	50
3.4.3	Configuración de extensiones.....	53
3.4.3.1	Configuración del teléfono.....	53
3.4.3.2	Configuración de la extensión.....	54
3.4.3.3	Configuración del directorio (End User).....	56
3.4.4	Enrutamiento de llamadas (Call Routing).....	57
3.4.4.1	Reglas de marcación (Dial Rules).....	59
3.4.4.2	Configuración de marcaciones externas (Route/Hunt).....	60
3.4.4.2.1	Route Group	61
3.4.4.2.2	Route List	61
3.4.4.2.3	Route Patterns.....	62
3.4.4.3	Configuración de los Hunt List y Line Groups	64
3.4.4.3.1	Line Group.....	65
3.4.4.3.2	Hunt List.....	68
3.4.4.3.3	Hunt Pilot.....	69
3.4.5	Trunk entre Cisco Call Manager y Asterisk	72
4	TELEFONÍA ASTERISK	76
4.1	Introducción.....	76
4.1.1	¿Qué es Asterisk?	76
4.1.2	Arquitectura de Asterisk.....	76
4.1.3	Integración de Asterisk con Cisco.....	77
4.1.4	Administración de Asterisk	79
4.1.5	Ficheros de configuración Asterisk.....	79

4.1.5.1	El archivo sip.conf.....	80
4.1.5.1.1	Clientes y servidores en sip.conf.....	81
4.1.5.2	El Dialplan.....	84
4.1.5.3	Las colas.....	87
4.2	Preparación del sistema.....	89
4.2.1	Hardware utilizado.....	89
4.2.2	Elección del software.....	90
4.2.3	Instalación CentOS.....	92
4.2.4	Instalación y configuración de Asterisk y FreePBX.....	96
4.2.5	Configuración MySQL.....	98
4.2.6	Instalación de FreePBX.....	99
4.2.7	Configuración inicial de FreePBX.....	100
4.2.8	Rotación de logs.....	101
4.2.9	Administración de FreePBX.....	102
4.3	Configuración de Asterisk mediante FreePBX.....	104
4.3.1	Configuración de las extensiones.....	104
4.3.2	Configuración de los troncales (Trunks).....	107
4.3.3	Configuración de las llamadas salientes (Outbound Routes).....	111
4.3.4	Configuración de Inbound Routes.....	114
4.3.5	Configuración Follow Me.....	114
4.3.6	Configuración Ring Groups.....	116
4.3.7	Otros servicios de Asterisk.....	117
4.3.7.1	IVR (Interactive Voice Responce).....	117
4.3.7.2	Blacklist.....	118
4.3.7.3	Queues.....	119
4.3.7.4	Time Group y Time Conditions.....	120
4.3.7.5	Conferences.....	121
4.3.7.6	Music on Hold (Música en espera).....	121
4.3.7.7	System Recording.....	122
4.3.8	Teléfonos y terminales.....	123
4.3.8.1	Teléfonos IP.....	123
4.3.8.2	Softphone.....	125
4.3.9	Flash Operador Channel (FOP).....	126
4.3.10	Report de llamadas.....	127

5	MONITORIZACIÓN CON NAGIOS	130
5.1	¿Qué es Nagios?	130
5.2	Instalación y configuración de SNMP en Asterisk.....	131
5.3	Configuración de Nagios para la monitorización de Asterisk.....	135
5.3.1	Script de comprobación de conexión de los trunks	135
5.3.2	Script de comprobación de conexión de Asterisk	139
5.4	Configuración SNMP en Cisco Call Manager	143
5.5	Configuración en Nagios para la monitorización de Cisco Call Manager ...	145
6	ANÁLISIS ECONÓMICO	150
6.1	Análisis económico de servidores	150
6.2	Análisis económico de los teléfonos IP.....	150
6.3	Análisis económico de la electrónica de red	150
6.4	Resumen comparativo de la inversión realizada para un centro	151
6.4.1	Inversión con Cisco	151
6.4.2	Inversión con Asterisk.....	151
6.4.3	Resultados.....	151
7	CONCLUSIONES Y FUTURO	152
7.1	Conclusiones.....	152
7.2	Futuro	153
8	BIBLIOGRAFÍA	154

1 INTRODUCCIÓN

La Telefonía IP es una tecnología que permite integrar en una misma red, basada en protocolo IP, las comunicaciones de voz y datos. Muchas veces se utiliza el término de redes convergentes o convergencia IP aludiendo a un concepto un poco más amplio de integración en la misma red de todas las comunicaciones (voz, datos, video, etc.).

Hasta ahora las empresas operaban con dos infraestructuras una para la señal de voz y otra para la señal de datos. Gracias al crecimiento en la velocidad de las comunicaciones de datos y a la aparición de nuevos protocolos es posible implementar la voz a través de la infraestructura de datos, de esta forma se puede reducir drásticamente los costes de telefonía.

Cuando hablamos de un sistema de telefonía IP estamos hablando de un conjunto de elementos que, debidamente integrados, permiten suministrar un servicio de telefonía (basado en VoIP) a la empresa, consiguiendo una infraestructura local de voz independiente de cualquier proveedor de telefonía, pudiendo realizar llamadas internas de manera gratuita.

Los elementos básicos que forman este sistema son: la centralita IP, el Gateway IP y los diferentes teléfonos IP.

Las principales ventajas de la telefonía IP son:

- la simplificación de la infraestructura de comunicaciones en la empresa.
- la integración de las diferentes sedes y trabajadores móviles de la organización en un sistema unificado de telefonía - con gestión centralizada, llamadas internas gratuitas, plan de numeración integrado y optimización de las líneas de comunicación.
- la movilidad y el acceso a funcionalidades avanzadas.

1.1 Objetivos

El objetivo de este proyecto es poder implantar telefonía IP en Labco España. Para ello, se instalarán: 2 Call Manager de Cisco, 2 Cisco Unity, unas 30 centralitas Gateway y unos 500 teléfonos. También instalaremos switches Cisco de nivel 2 y de nivel 3.

Para ello, instalaremos centralitas Cisco con la ayuda de la consultora Sirt en los principales centros de la compañía y en los centros más pequeños instalaremos solamente teléfonos IP que se conectarán a una centralita Asterisk configurada por nosotros. Asterisk es un programa GPL con el cual conseguimos montar una centralita PBX gratis en cualquier servidor que queramos.

El objetivo principal en el que se basa este proyecto es el poder realizar llamadas entre las distintas centralitas de modo que sea transparente para el usuario que realice la llamada.

Una vez logrado esto, conseguiremos reducir drásticamente la factura telefónica de la compañía, pasando de una telefonía analógica en la que se paga la línea y las llamadas realizadas a una telefonía digital en la que solamente se paga la línea ADSL.

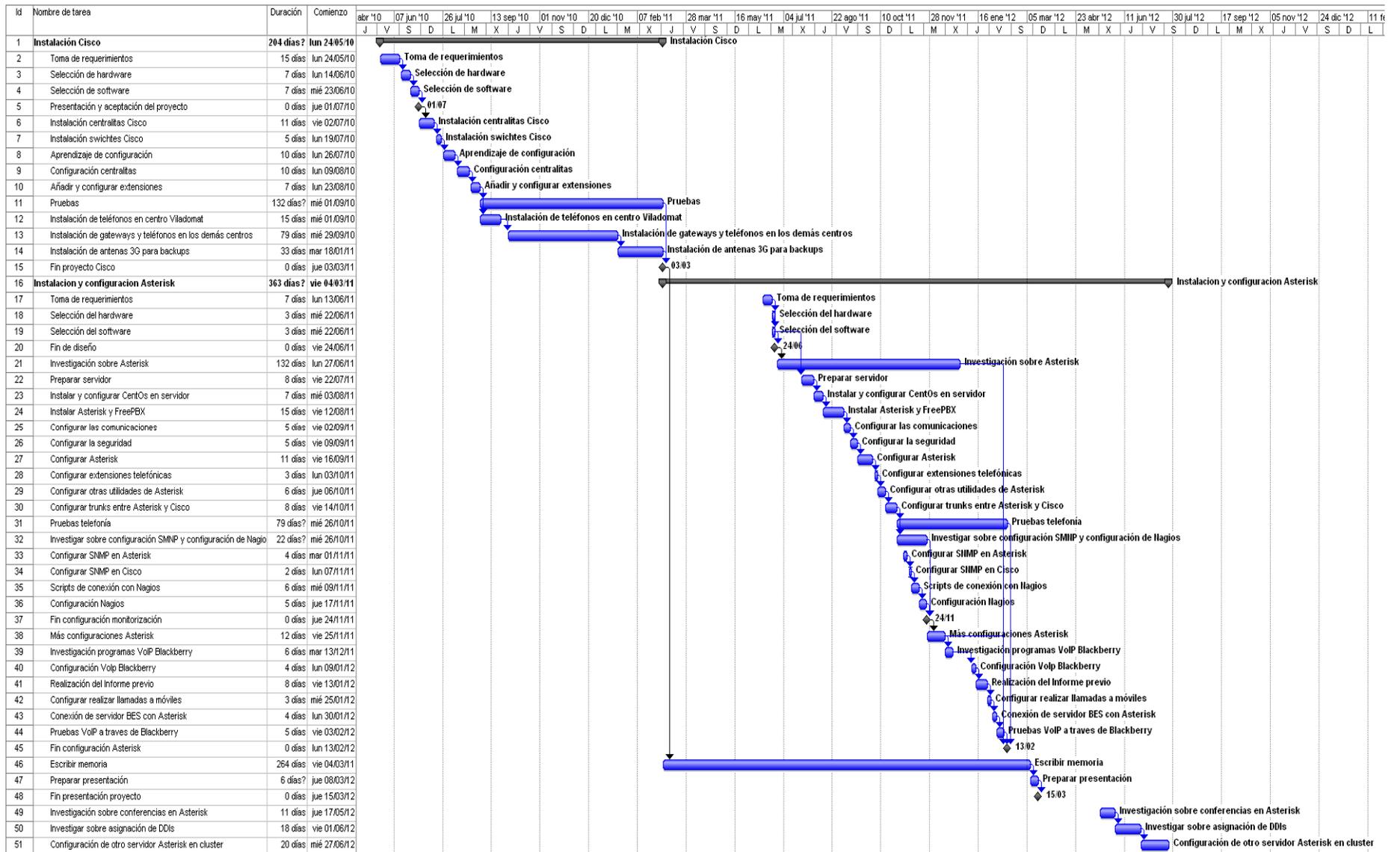
La integración de Cisco da lugar a una gran reducción de costes, aunque para centros pequeños no sale a cuenta montar una estructura Cisco con sus switches, ASAs y teléfonos ya que el alto coste de estos elementos no lo compensa. Por ese motivo hemos decidido implantar Cisco en los centros con mucho volumen y utilizar la centralita Asterisk para los centros con menos usuarios.

1.2 Planificación

El comienzo del proyecto comienza con la instalación de toda la telefonía de Cisco. Esta instalación comienza el día 24 de mayo del año 2010.

El comienzo del estudio e implantación de Asterisk comienza el día 13 de junio de 2011. El proyecto finaliza el día 15 de marzo de 2012.

La siguiente imagen muestra el diagrama de Gantt del proyecto.



2 CONCEPTOS GENERALES

2.1 VoIP

2.1.1 ¿Qué es VoIP?

La Voz sobre IP (VoIP, Voice over IP) es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos.

La Telefonía IP es una aplicación inmediata de esta tecnología, de forma que permita la realización de llamadas telefónicas ordinarias sobre redes IP u otras redes de paquetes utilizando un PC, gateways y teléfonos estándares. En general, servicios de comunicación - voz, fax, aplicaciones de mensajes de voz - que son transportados vía redes IP, Internet normalmente, en lugar de ser transportados vía la red telefónica convencional.

La VoIP (Voz sobre IP) esta sigla designa la tecnología empleada para enviar información de voz en forma digital en paquetes a través de los protocolos de Internet, en vez de hacerlo a través de la red de telefonía habitual, además es una tecnología de telefonía que puede ser habilitada a través de una red de datos de conmutación de paquetes. La ventaja real de esta tecnología es la transmisión de voz de forma gratuita, ya que viaja como datos.

Con VoIP podemos conseguir:

- Acceso a las redes corporativas desde pequeñas sedes a través de redes integradas de voz y datos conectadas a sucursales.
- Directorios corporativos basados en la Intranet con servicios de mensajes y números personales para quienes deben desplazarse.
- Servicios de directorio y de conferencias basadas en gráficos desde el sistema de sobremesa.
- Redes privadas y gateways virtuales gestionados para voz que sustituyen a las Redes Privadas Virtuales (VPN).

2.1.1.1 Ventajas de VoIP

- **Menor coste.** La primera ventaja y la más importante es el coste, una llamada mediante VoIP es mucho mas barata que su equivalente en telefonía convencional. Esto es básicamente debido a que se utiliza la misma red para la transmisión de datos y voz, la telefonía convencional tiene costos fijos que la telefonía IP no tiene, de ahí que ésta es mas barata. Usualmente para una llamada entre dos teléfonos IP la llamada es gratuita, cuando se realiza una llamada de un teléfono IP a un teléfono convencional el costo corre a cargo del teléfono IP.
- **Portátil.** Con VoIP se puede realizar una llamada desde cualquier lado que exista conectividad a Internet. Dado que los teléfonos IP transmiten su información a través de Internet estos pueden ser administrados por su proveedor desde cualquier lugar donde exista una conexión. Esto es una ventaja para las personas que suelen viajar mucho, estas personas pueden llevar su teléfono consigo siempre teniendo acceso a su servicio de telefonía IP.
- **Libre de características adicionales.** VoIP viene con varias características que los teléfonos regulares tienen también. Pero éste les ofrece por un precio de VoIP al mismo tiempo les ofrece de forma gratuita. Si se está usando un teléfono regular, y se quiere actualizar a fin de que haya transferencia de llamadas, correo de voz y llamada en espera entonces se tiene que pagar cargos adicionales para su instalación. Con el VoIP estas características ya vienen con el sistema sin costo alguno.

2.1.1.2 Desventajas de VoIP

- **La VoIP requiere conexión eléctrica.** Es necesario tener energía eléctrica para que VoIP funcione. Con la telefonía convencional éste problema no se da ya que la energía la cogen de la electricidad que fluye a través de la red telefónica, por lo que si hay un corte de energía y no tenemos el servidor conectado a algún SAI podemos quedarnos sin telefonía.
- Dado que VoIP utiliza una conexión de red, la calidad del servicio se ve afectado por **la calidad de esta línea de datos**, esto quiere decir que la calidad

de una conexión VoIP se puede ver afectada por problemas como la alta latencia (tiempo de respuesta) o la pérdida de paquetes. Las conversaciones telefónicas se pueden ver distorsionadas o incluso cortadas por este tipo de problemas. Es indispensable para establecer conversaciones VoIP satisfactorias contar con una cierta estabilidad y calidad en la línea de datos.

- **Ataques.** La VoIP es susceptible de ser atacada por virus y hackers.

2.1.2 Elementos necesarios en una red VoIP

Hay tres elementos imprescindibles en una red de VoIP:

- **El cliente o terminal:** Este elemento establece y termina las llamadas de voz. Codifica, empaqueta y transmite la información de salida generada por el micrófono del usuario. Asimismo, recibe, decodifica y reproduce la información de voz de entrada a través de los altavoces o audífonos del usuario. Se pueden implementar tanto en software como en hardware.
- **Gatekeepers:** El segundo elemento de la Voz sobre IP son los sustitutos de las centralitas convencionales, los cuales manejan un amplio rango de operaciones complejas de bases de datos, tanto en tiempo real como fuera de él. Estas operaciones incluyen validación de usuarios, tasación, contabilidad, tarificación, recolección, distribución de utilidades, enrutamiento, administración general del servicio, carga de clientes, control del servicio, registro de usuarios y servicios de directorio entre otros.
- **Gateways:** El tercer elemento lo conforman los gateways de Voz sobre IP, los cuales proporcionan un puente de comunicación entre los usuarios. se trata del enlace con la red telefónica tradicional, actuando de forma transparente para el usuario. Estos equipos también juegan un papel importante en la seguridad de acceso, la contabilidad, el control de calidad del servicio (QoS; Quality of Service) y en la mejora del mismo.

2.1.3 Protocolos de VoIP

Los protocolos son los lenguajes que utilizarán los distintos dispositivos VoIP para su conexión. Esta parte es importante ya que de ella dependerá de la eficacia, la complejidad y la sincronización de la comunicación.

Vamos a ver los 3 protocolos más extendidos en VoIP:

- Protocolo SIP
- Protocolo SCCP
- Protocolo H.323
- Protocolo IAX

2.1.3.1 SIP

El protocolo SIP (Session Initiation Protocol) fue desarrollado por el grupo MMUSIC (Multimedia Session Control) del IETF, definiendo una arquitectura de señalización y control para VoIP.

El propósito de SIP es la comunicación entre dispositivos multimedia. SIP hace posible esta comunicación gracias a dos protocolos que son RTP¹/RTCP y SDP.

El protocolo RTP se usa para transportar los datos de voz en tiempo real, mientras que el protocolo SDP se usa para la negociación de las capacidades de los participantes, tipo de codificación, etc.

SIP fue diseñado de acuerdo al modelo de Internet. Es un protocolo de señalización extremo a extremo que implica que toda la lógica es almacenada en los dispositivos finales (salvo el enrutado de los mensajes SIP). El estado de la conexión es también almacenado en los dispositivos finales. El precio a pagar por esta capacidad de distribución y su gran escalabilidad es una sobrecarga en la cabecera de los mensajes producto de tener que mandar toda la información entre los dispositivos finales.

¹ RTP son las siglas de Real-time Transport Protocol (Protocolo de Transporte de Tiempo real). Es un protocolo de nivel de sesión utilizado para la transmisión de información en tiempo real, como por ejemplo audio y vídeo en una video-conferencia.

SIP es un protocolo de señalización a nivel de aplicación para establecimiento y gestión de sesiones con múltiples participantes. Se basa en mensajes de petición y respuesta y reutiliza muchos conceptos de estándares anteriores como HTTP y SMTP.

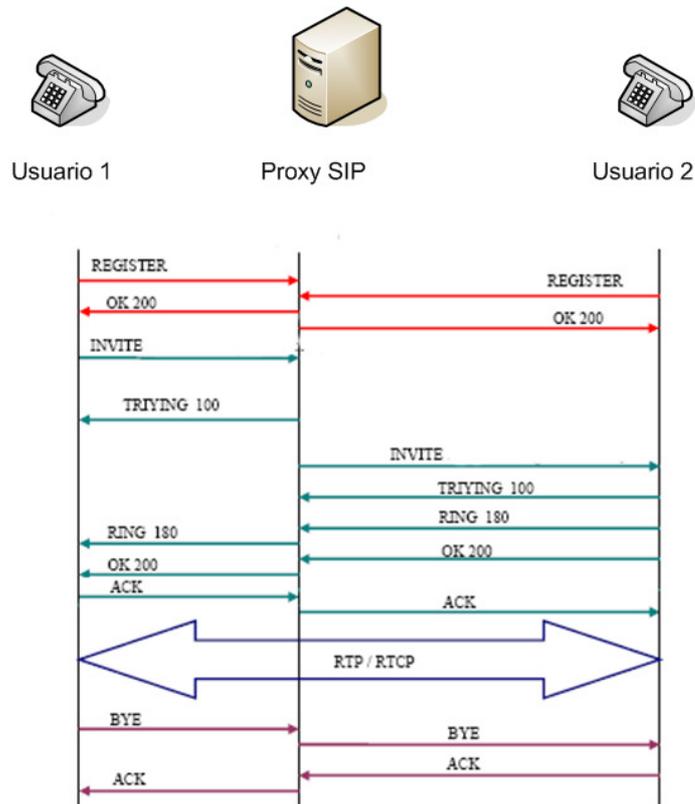
- Ventajas:
 - Es el protocolo estándar de la telefonía IP y esta ampliamente extendido entre los principales fabricantes de telefonía IP.
- Inconvenientes:
 - Problemas de NAT. En SIP la señalización y los datos viajan de manera separada y por eso aparecen problemas de NAT en el flujo de audio cuando este flujo debe superar los routers y firewalls. SIP suele necesitar un servidor STUN² para estos problemas.
 - Utilización de puertos. SIP utiliza un puerto (5060) para señalización y 2 puertos RTP por cada conexión de audio (como mínimo 3 puertos). Si tenemos 100 llamadas simultáneas con SIP se usarían 200 puertos (RTP) más el puerto 5060 de señalización.

² Un servidor STUN (Simple Traversal of User Datagram Protocol [UDP] a través de Network Address Translators [NATs]), permite a los clientes NAT (tal como computadores detrás de un firewall), configurar llamadas telefónicas a un proveedor VOIP alojado afuera de su red local.

El servidor STUN permite a los clientes encontrar sus direcciones públicas, el tipo de NAT del cual ellos están atrás y el puerto Internet asociado por el NAT con el puerto local específico. Esta información es usada para configurar comunicación UDP entre el cliente y el proveedor VOIP para así establecer una llamada.

2.1.3.1.1 Comunicación SIP

A continuación vemos un gráfico de qué es lo que ocurre durante una llamada a través del protocolo SIP:



En una llamada SIP hay varias transacciones SIP. Una transacción SIP se realiza mediante un intercambio de mensajes entre un cliente y un servidor:

- Las dos primeras transacciones corresponden al registro de los usuarios. Los usuarios deben registrarse para poder ser encontrados por otros usuarios. En este caso, los terminales envían una petición REGISTER, donde los campos from y to corresponden al usuario registrado. El servidor Proxy, que actúa como Register, consulta si el usuario puede ser autenticado y envía un mensaje de OK en caso positivo.
- La siguiente transacción corresponde a un establecimiento de sesión. Esta sesión consiste en una petición INVITE del usuario al proxy. Inmediatamente, el proxy envía un TRYING 100 para parar las retransmisiones y reenvía la petición al usuario B. El usuario B envía un Ringing 180 cuando el teléfono empieza a

sonar y también es reenviado por el proxy hacia el usuario A. Por último, el OK 200 corresponde a aceptar la llamada (el usuario B descuelga).

- En este momento la llamada está establecida, pasa a funcionar el protocolo de transporte RTP con los parámetros (puertos, direcciones, codecs, etc.) establecidos en la negociación mediante el protocolo SDP.
- La última transacción corresponde a una finalización de sesión. Esta finalización se lleva a cabo con una única petición BYE enviada al Proxy, y posteriormente reenviada al usuario B. Este usuario contesta con un OK 200 para confirmar que se ha recibido el mensaje final correctamente.

2.1.3.2 SCCP

El protocolo SCCP (Skinny Client Control Protocol), es un protocolo propietario de Cisco, el cual realiza la señalización entre el Call Manager y los teléfonos IP. Un cliente skinny utiliza TCP/IP para conectarse a los Call Managers y así poder transmitir las llamadas. Para transportar el audio utiliza RTP, UDP e IP.

2.1.3.3 H.323

H.323 es una recomendación del ITU-T (International Telecommunication Union), que define los protocolos para proveer sesiones de comunicación audiovisual sobre paquetes de red.

H.323 es utilizado comúnmente para Voz sobre IP y para videoconferencia basada en IP. Es un conjunto de normas ITU para comunicaciones multimedia que hacen referencia a los terminales, equipos y servicios estableciendo una señalización en redes IP. No garantiza una calidad de servicio, y en el transporte de datos puede, o no, ser fiable; en el caso de voz o vídeo, nunca es fiable. Además, es independiente de la topología de la red y admite pasarelas, permitiendo usar más de un canal de cada tipo (voz, vídeo, datos) al mismo tiempo.

H.323 está definido de tal manera que las empresas que manufacturan los equipos pueden agregar sus propias especificaciones al protocolo y pueden definir otras estructuras de estándares que permiten a los dispositivos adquirir nuevas clases de características o capacidades.

2.1.3.4 IAX

El protocolo IAX (Inter-Asterisk eXchange protocol) fue diseñado como un protocolo de conexiones VoIP entre servidores Asterisk aunque hoy en día también sirve para conexiones entre clientes y servidores que soporten el protocolo.

- Ventajas
 - Consume menos ancho de banda que SIP, ya que IAX es un protocolo binario en lugar de ser un protocolo de texto como SIP y además intenta reducir al máximo las cabeceras de los mensajes.
 - Para evitar los problemas de NAT el protocolo IAX usa como protocolo de transporte UDP, normalmente sobre el puerto 4569, y tanto la información de señalización como los datos viajan conjuntamente (a diferencia de SIP) y por tanto lo hace menos proclive a problemas de NAT y le permite pasar los routers y firewalls de manera más sencilla.
- Inconvenientes
 - No está extendido entre los fabricantes de hardware y software

2.1.3.5 Otros protocolos

- Megaco (También conocido como H.248) y MGCP - Protocolos de control
- UNISTim - Protocolo propiedad de Nortel
- MiNet - Protocolo propiedad de Mitel
- CorNet-IP - Protocolo propiedad de Siemens
- Skype - Protocolo propietario peer-to-peer utilizado en la aplicación Skype
- Jingle - Protocolo abierto utilizado en tecnología XMPP
- MGCP- Protocolo propietario de Cisco
- weSIP- Protocolo licencia gratuita de VozTelecom

2.1.4 Parámetros VoIP

2.1.4.1 Códecs

La comunicación de voz es analógica, mientras que la red de datos es digital. El proceso de convertir ondas analógicas a información digital se hace con un codificador-decodificador (el CODEC). Hay muchas maneras de transformar una señal de voz analógica, todas ellas gobernadas por varios estándares. El proceso de la conversión es complejo. Es suficiente decir que la mayoría de las conversiones se basan en la modulación codificada mediante pulsos (PCM) o variaciones.

Además de la ejecución de la conversión de analógico a digital, el CODEC comprime la secuencia de datos, y proporciona la cancelación del eco. La compresión de la forma de onda representada puede permitir el ahorro del ancho de banda. Esto es especialmente interesante en los enlaces de poca capacidad y permite tener un mayor número de conexiones de VoIP simultáneamente. Otra manera de ahorrar ancho de banda es el uso de la supresión del silencio, que es el proceso de no enviar los paquetes de la voz entre silencios en conversaciones humanas.

Entre los codecs más utilizados en VoIP encontramos:

- G.711: bit-rate de 56 o 64 Kbps.
- G.723: bit-rate de 5,3 o 6,4 Kbps.
- G.729: bit-rate de 8 o 13 Kbps.

2.1.4.2 QoS

Los problemas de la calidad del servicio en VoIP vienen derivados principalmente por dos factores:

- 1) Internet es un sistema basado en conmutación de paquetes y por tanto la información no viaja siempre por el mismo camino. Esto produce efectos como la pérdida de paquetes o el jitter.

- 2) Las comunicaciones VoIP son en tiempo real lo que produce que efectos como el eco, la pérdida de paquetes y el retardo o latencia sean muy molestos y perjudiciales y deban ser evitados.

Los principales problemas en cuanto a la calidad del servicio (QoS) de una red de VoIP son:

- **Latencia:** La latencia se define técnicamente en VoIP como el tiempo que tarda un paquete en llegar desde la fuente al destino. El valor recomendado entre el punto inicial y final de la comunicación debiera ser inferior a 150 ms.
- **Jitter:** El jitter se define técnicamente como la variación en el tiempo en la llegada de los paquetes, causada por congestión de red, pérdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino. El valor recomendado entre el punto inicial y final de la comunicación debiera ser inferior a 100 ms.
- **La pérdida de paquetes:** Las comunicaciones en tiempo real están basadas en el protocolo UDP. Este protocolo no está orientado a conexión y si se produce una pérdida de paquetes no se reenvían. Sin embargo la voz es bastante predictiva y si se pierden paquetes aislados se puede recomponer la voz de una manera bastante óptima. La pérdida de paquetes máxima admitida para que no se degrade la comunicación deber ser inferior al 1%.
- **Eco:** El eco se produce por un fenómeno técnico que es la conversión de 2 a 4 hilos de los sistemas telefónicos o por un retorno de la señal que se escucha por los altavoces y se cuela de nuevo por el micrófono. El eco también se suele conocer como reverberación.
- **Ancho de banda:** En conexiones a Internet el ancho de banda se define técnicamente como la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bites por segundo (BPS), kilobites por segundo (kbps), o megabites por segundo (mps).

2.1.5 VoIP en el modelo OSI

La siguiente tabla muestra la relación entre el modelo OSI (Open System Interconnection) y los protocolos usados por VoIP.

Niveles OSI	Protocolos VoIP
7 Aplicación	Asterisk, Aplicaciones
6 Presentación	G.729, G.723, G.711, GSM
5 Sesión	H.323, MGCP, SIP, IAX
4 Transporte	RTP, TCP, UDP
3 Red	IP
2 Enlace de Datos	Frame Relay, ATM, Ethernet, PPP, MLP
1 Físico	Ethernet, V.35, RS-232, xDSL

Como podemos ver en la figura de arriba, la voz sobre IP esta compuesta de diversos protocolos que envuelven varios niveles del modelo OSI. Principalmente trata las capas de transporte, sesión, presentación y aplicación.

En la capa de transporte, la mayor parte de estos protocolos usa RTP/RTCP, siendo el primero un protocolo de media y el segundo un protocolo de control. Todos ellos utilizan UDP para transportar la voz.

En la capa de sesión entran los protocolos de voz sobre IP propiamente dichos, H323, SIP, IAX etc.

En la capa de sesión los Códecs definen el formato de presentación de voz con sus diferentes variaciones de compresión.

3 TELEFONÍA CISCO

El primer paso de este proyecto consiste pasar toda la telefonía analógica de Labco a una telefonía IP con tecnología de Cisco y con comunicaciones de Telefónica.

Para la integración de la telefonía IP estaremos asesorados por la consultora Sirt en colaboración con Telefónica.

3.1 La telefonía IP de Cisco

Para conseguir tener telefonía IP utilizaremos lo que en Cisco denominan como “Comunicaciones Unificadas de Cisco”. Esto es un sistema de comunicaciones IP de productos y aplicaciones de voz, vídeo, datos y movilidad. Permite que las comunicaciones sean más eficaces y seguras consiguiendo un efecto directo en el incremento de la facturación y la rentabilidad. Crea una nueva forma de comunicación que da movilidad a la empresa y hace que la información se encuentre siempre disponible, en cualquier momento y desde cualquier lugar. Las Comunicaciones Unificadas de Cisco forman parte de una solución integrada que incluye infraestructura de red, seguridad, movilidad, productos de administración de red, servicios de tipo lifecycle, opciones flexibles de implementación y administración, además de aplicaciones de comunicaciones de terceros.

Los componentes principales de Comunicaciones Unificadas de Cisco son:

- Telefonía IP
 - Software de procesamiento de llamadas
 - Teléfonos y terminales
- Aplicaciones de Comunicaciones Unificadas de Cisco
 - Clientes de comunicaciones unificadas
 - Mensajería
 - Conferencia multimedia
- Infraestructura de Comunicaciones de Cisco

3.2 Tecnología utilizada en la telefonía IP

3.2.1 Centralitas

Para conseguir realizar la conexión y configuración de la telefonía IP con tecnología Cisco utilizaremos:

Cisco Unified Communications Manager 7.1

Son los servidores que hacen de centralita. Aquí entre otras cosas se configuran las extensiones, su comportamiento y los permisos de llamada de cada una.

En nuestro caso tenemos dos Communications Manager, también llamados Call Manager, agrupados en clústeres, los cuales se gestionan como una única entidad en nuestra red IP. Los Call Manager permiten una escalabilidad desde 1 hasta 30.000 teléfonos IP por clúster y el equilibrado de carga y redundancia en servicio de procesamiento de llamadas, lo que significa un mejor rendimiento y que todas las llamadas no las procese un único Call Manager.

Las características funcionales de centralita de Cisco Unified Callmanager son:

- Retrollamada
- Desvío incondicional
- Desvío si no contesta
- Desvío si ocupado
- Llamada en espera
- Capturas de llamada
- Aparcamiento de llamadas
- Transferencias
- Conferencias
- Grupos de salto
- Música en espera
- Servicio Nocturno

- Intercomunicador
- Bloqueos de llamada
- Monitorización de líneas
- Red única de voz y datos
- Buzón de voz / Mensajería Integrada con correo
- Operadora Automática

3.2.2 Teléfonos y terminales

Cisco IP Phone 7911G

Terminal utilizado para los puestos de trabajo fijos.

7911G		<p>Switch integrado, 2 puertos 10/100 1 tecla de línea 4 teclas de funcionalidad programables Modo monitor LED de indicación de mensaje de voz Acceso a aplicaciones XML PoE Teclado alfabético</p>
-------	---	--

Cisco IP Phone 7962G

Terminal utilizado para utilizarlo como centralita de recepción de llamadas. A este terminal se le pueden añadir pantallas laterales donde aparecen las extensiones que configuremos a través del Call Manager para tenerlas directamente y poder pasar llamadas más fácilmente.

7962G		<p>Pantalla 320x222 píxeles, escala en grises 4-bit profundidad</p> <p>Switch integrado, 2 puertos 10/100</p> <p>6 teclas de línea luminosas</p> <p>4 teclas de funcionalidad programables</p> <p>Manos libres</p> <p>LED de indicación de mensaje de voz</p> <p>Acceso a aplicaciones XML</p> <p>PoE</p> <p>Teclado alfabético</p> <p>Posibilidad de expansión de líneas con módulo 7914</p> <p>Wireless Headset</p> <p>Soporte Wideband</p>
Módulo de expansión 7915/16		Módulo de expansión de 14 líneas para las series 7962

Cisco Wireless IP Phone 7921G

Terminal inalámbrico utilizado para los usuarios que necesitan movilidad. Una vez montado el sistema, estos usuarios podrán ir con el teléfono a cualquier centro y el teléfono funcionará con la misma extensión.

7921G y		7921G Teléfono Wireless
---------	---	-------------------------

Cisco Aironet 1130G Serie IEEE 802.11g Acces Point

Antena que da cobertura y conexión a los teléfonos inalámbricos 7921G y los conecta a la red de la sede en la que se encuentre para poder realizar y recibir las llamadas.

Dichas antenas deberán estar dispuestas en cada sede de tal forma que podamos tener cobertura en todos los puntos del laboratorio.

Aironet 1130G		1130G Antena Wireless
------------------	---	-----------------------

Cisco ATA 186 Analog Adapter

Cualquier aparato analógico se conecta a los ATA's para así transformar la señal analógica en digital. Básicamente se conectan los faxes y los teléfonos analógicos.

ATA 186		ATA 186 Analog Adapter
---------	---	------------------------

Cisco IP Communicator (SoftPhone de Cisco)

Es un programa el cual podemos utilizar en cualquier ordenador con Windows. Una vez instalado nos aparece un teléfono en la pantalla el cual funciona como si fuera una extensión más.

IP Comunica tor		8 teclas de línea luminosas 5 teclas de funcionalidad programables Manos libres LED de indicación de mensaje de voz Acceso a aplicaciones XML Teclado alfabético
-----------------------	---	---

3.3 Las comunicaciones

3.3.1 Punto de partida

En estos momentos tenemos interconectadas las sedes mediante conexiones Net-LAN³.

3.3.2 Nuevas comunicaciones

Atendiendo a los requerimientos del proyecto se ha decidido implementar una solución basada sobre el servicio MacroLAN⁴ y VPNIP⁵ creando nuestra propia red privada virtual.

Este cambio de conexiones afecta a 57 sedes de la empresa en las que se creará una RPV⁶ con las siguientes configuraciones:

SEDE CENTRAL

- 1 Acceso 100 Mbps
- 1 Acceso 100 Mbps diversificado de backup

³ Net-LAN ofrece mediante conexiones ADSL, RDSI o accesos punto a punto, la creación de una RPV (Red Privada Virtual), es decir, poder trabajar con todas las sedes de la empresa como si estuviéramos en una intranet.

⁴ MacroLAN, o antiguamente conocido como MetroLAN, es un servicio de redes privadas virtuales (VPN) Ethernet de ámbito metropolitano que se ofrece a empresas y que permite disponer de acceso de banda ancha (del orden de Gbps) mediante fibra óptica.

Con el servicio MacroLAN, es posible interconectar la red de área local de una empresa de tal forma que todas las computadoras parecen estar interconectadas en un mismo segmento de LAN. De esta forma, los empleados que están ubicados lejos de la central empresarial, pueden comunicarse entre sí y acceder a los servidores remotos tan fácilmente como si los empleados y servidores se localizaran en el mismo edificio.

⁵ El Servicio VPN-IP (Redes Privadas Virtuales IP) es el servicio gestionado de interconexión de redes basado en el protocolo IP/MPLS, que permite la implementación de redes privadas virtuales para enlazar a los diferentes puntos de las empresas a través de las diferentes redes públicas del ICE: Red IP, Red-ATM etc., de manera segura y confiable manteniendo la misma prestación del servicio como si fuera un segmento de red privada de área local del cliente.

⁶ Red Privada Virtual

- 1 Caudal Metro⁷ Plata de 100 Mbps
- 2 Switch Cisco 3560-24TS en alquiler con gestión y mantenimiento avanzado

4 SEDES FIBRA OPTICA + BACK UP ACCESO 2 M

- 4 Accesos 10 Mbps
- 4 Caudal Metro Plata de 10 Mbps
- 4 Accesos Cobrelan⁸ Backup 2 Mbps
- 8 Router Cisco 2801 en alquiler con gestión y mantenimiento avanzado

5 SEDES ACCESO 2 Mbps + BACK UP SDSL SIMETRICA 1 Mbps

- 5 Accesos Cobrelan 2 Mbps
- 5 Accesos Back up ADSL Simétrica 1 Mbps
- 5 Router Cisco 2801 en alquiler con gestión y mantenimiento avanzado
- 5 Router Cisco 877-M en alquiler con gestión y mantenimiento avanzado

2 SEDES ACCESO 2 Mbps + BACK UP ADSL MAXIMA 3 Mbps

- 2 Accesos Cobrelan 2 Mbps
- 2 Accesos Back up ADSL Máxima 3 Mbps
- 2 Router Cisco 2801 en alquiler con gestión y mantenimiento avanzado
- 2 Router Teldat C1i+ en alquiler con gestión y mantenimiento avanzado

45 DELEGACIONES VPNIP SOBRE ACCESO ADSL

- Accesos ADSL Máxima 3 Mbps/1 Mbps
- Prolongación de cableado
- Mantenimiento plata de los accesos ADSL
- Caudal 100% Plata ADSL Máxima
- Router's Teldat C1i+ en alquiler con gestión y mantenimiento avanzado

CAUDALES NACIONALES

⁷ La Red Metro Ethernet, es una arquitectura tecnológica destinada a suministrar servicios de conectividad MAN/WAN de nivel 2, a través de UNIs Ethernet. Estas redes denominadas "multiservicio", soportan una amplia gama de servicios, aplicaciones, contando con mecanismos donde se incluye soporte a tráfico "RTP" (tiempo real), como puede ser Telefonía IP y Video IP, este tipo de tráfico resulta especialmente sensible a retardo, al jitter y al grudge.

⁸ ADSL a 2Mbps

- Caudal Nacional Agregado Plata de 40 Mbps en MAN⁹ Barcelona
- Caudal Nacional Agregado Plata de 10 Mbps en MAN Madrid

3.3.3 Tecnología utilizada para la conexión

Los routers y switches que se han instalado para las comunicaciones son:

Switch Cisco Catalyst 3750 Metro Series

Los switches de la serie Cisco Catalyst 3750 es una línea de productos que mejora la eficiencia de funcionamiento LAN al combinar una facilidad de uso con la alta resistencia para switches apilables. Esta serie de productos cuenta con la tecnología Cisco StackWise, una interconexión de pilas de 32 Gbps que permite crear un sistema de conmutación unificado y altamente resistente. Esta pensado para organizaciones de tamaño medio y sucursales.



Router Cisco 2801

Las características principales son:

- Seguridad a través de hasta 800 túneles VPN, IOS FW, NAC, IPS o de seguridad de contenido.
- Voz: media/alta densidad analógico/digital de voz con correo de voz de telefonía IP, Call Manager Express o capacidad de supervivencia para hasta 24 teléfonos.
- Alto rendimiento de seguridad concurrente, voz y servicios avanzados.
- Integración de doble puertos 10/100



⁹ Metropolitan Area Network

Router Cisco 877

Las series 870 de Cisco soportan múltiples tipos de servicios DSL, cable y conexiones Metro Ethernet en pequeñas oficinas. Proporcionan el rendimiento adecuado para soportar varios procesos paralelos como firewall,



detección de intrusiones y encriptación por VPN. Como opción también pueden llevar Wi-Fi y están especialmente diseñados para ofrecer una calidad de servicio (QoS) optimizada para transportar paquetes de voz y de video.

El modelo 877 soporta ADSL sobre RDSI para poder utilizar una RDSI de backup.

Router Teldat C1+L

El router Teldat C1+L soluciona de una forma sencilla y eficaz la conectividad a la red corporativa o internet con banda ancha sobre accesos ADSL/ADSL2+, y



opcionalmente a través de redes 3.5G. La conectividad 3.5G comprende todas las tecnologías de conectividad móvil desplegadas (HSPA, UMTS, EDGE, GPRS, GSM, CDMA y TD-SCDMA). El nuestro caso utilizaremos la conectividad mediante ADSL2+ y backup 3.5G en caso de caída del acceso ADSL. Además, estos routers cuentan con un switch de 4 puertos 10/100 y opción WiFi.

3.3.4 Interconexión de sedes

Para interconectar las sedes entre sí y que los teléfonos IP de cada una de ellas puedan realizar llamadas y tener una extensión hemos decidido implementar una conexión centralizada, es decir, el gestor de llamadas, en nuestro caso el Call Manager, esta localizado en la sede central y todos los teléfonos, tanto de las sedes remotas como los de la central, se registran en él.

¿Qué pasa si falla la conexión VPNIP?

El centro tiene un backup con conexión 3G. Los teléfonos seguirían trabajando por esa conexión sin cables a través de unas antenas instaladas estratégicamente para poder tener dicha conexión.

¿Qué pasa si el Call Manager principal deja de funcionar?

Pasaríamos a modo supervivencia. Los teléfonos pasarían a registrarse al Call Manager de backup situado en Madrid, permitiendo realizar las llamadas sin que el usuario note que ha habido un fallo en el sistema.

Los Call Manager se ubican en ciudades distintas para evitar quedarnos sin Call Manager que nos permitan comunicarnos por si hay un corte generalizado de electricidad en alguna ciudad, evitar dejar a todo el grupo sin teléfonos en toda España.

¿Qué pasa si fallan los dos Call Manager?

Los gateways que hay en los centros cogerían la administración de las llamadas hacia el exterior. En este caso no podrán realizarse llamadas a extensiones que estén ubicadas fuera de esa sede pero si podrían realizarse llamadas por números de teléfono convencionales. Como todos los centros tienen como mínimo un primario con un número de teléfono convencional, podemos tener todavía comunicación telefónica.

3.3.5 Seguridad en las conexiones

Para separar las comunicaciones y que cada servicio opere por separado hemos creado diferentes VLANs¹⁰ en los switches de cada centro.

En cada centro hay las siguientes VLANs:

- **LAN de Datos:** VLAN 1: 10.34.x.0/24, donde x es un octeto diferente para cada centro. En esta VLAN están conectados los ordenadores e impresoras.

¹⁰ VLAN es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único switch físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local.

- **LAN de Voz:** VLAN 100: 10.1.x.0/24, donde x es un octeto diferente para cada centro. Esta VLAN es la de telefonía IP y cada teléfono de cada centro cogerá una IP de esta VLAN. En esta VLAN también están ubicadas las centralitas telefónicas de Cisco.
- **LAN de invitados:** VLAN 20: 10.2.0.0/24: esta VLAN es la wireless de cada centro.

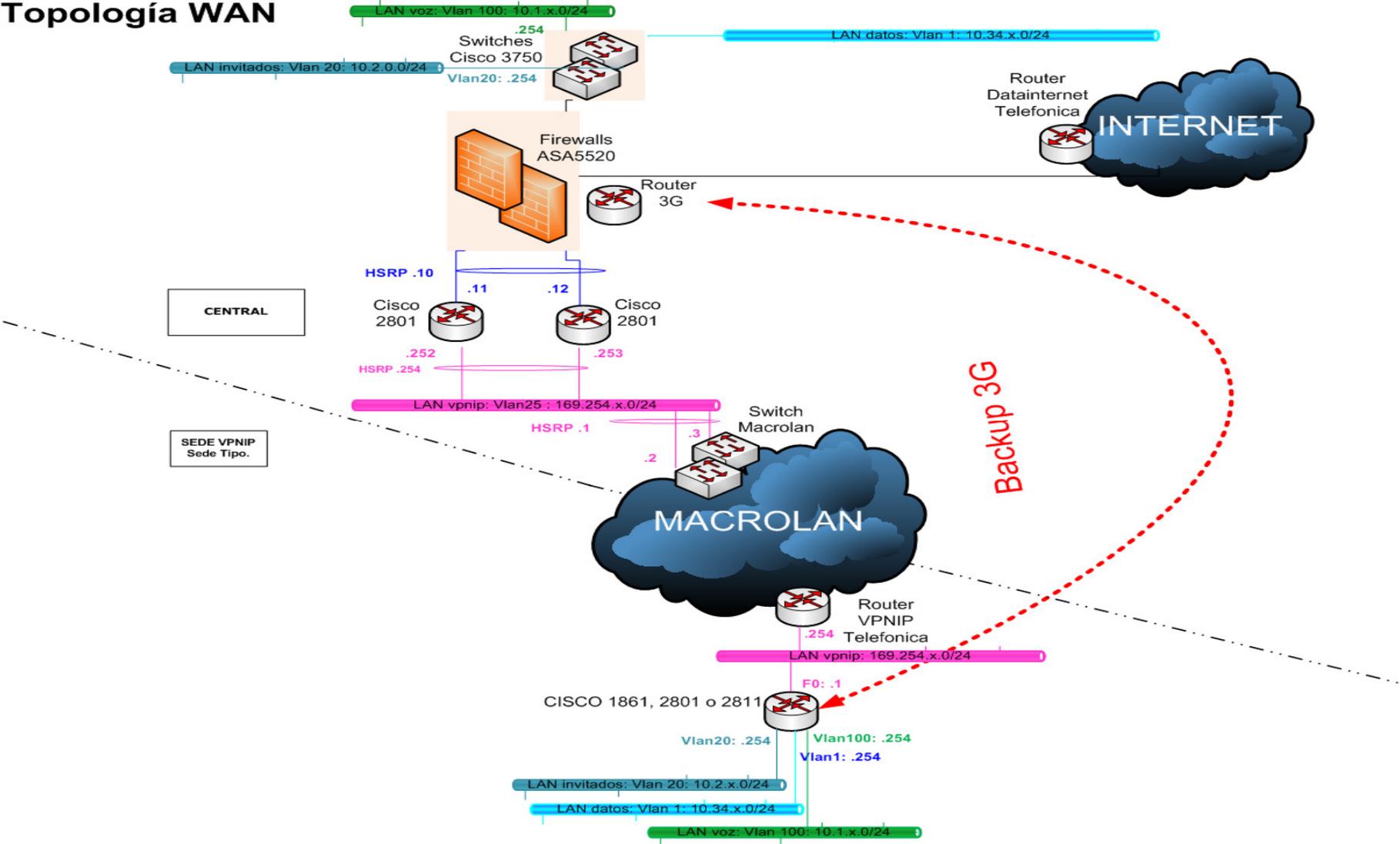
3.3.6 Topología de la red

En esta sección se explica la topología de red de la red WAN y de las diferentes sedes tipo.

Utilizaremos la siguiente leyenda para los diferentes componentes de la red:

- RO – Router
- SW – Switch
- GW – Gateway de voz
- VG – Gateway y FXS (Extensiones Analógicas)
- CM – Cisco Unified Call Manager
- UCN – Cisco Unity Connection
- CO – Controler Wireless
- FW – Firewall

Topología WAN



En la figura anterior podemos ver la topología de red de la WAN.

En la parte de arriba vemos todo el hardware de red necesario para hacer la conexión de la sede central (en Barcelona) y en la parte de abajo vemos como están conectadas las demás sedes.

Podemos ver que en ambas sedes tenemos las mismas VLANs. En la sede central una vez dentro de la red tenemos los dos switches Cisco 3750 de nivel 3 que nos conmutan el tráfico de la red.

Si algún paquete tiene que salir fuera de esta red local, es enrutado por los routers Cisco 2801, donde configuramos que todo paquete que tenga que salir por la MacroLan lo haga por los dos switches de MacroLan que vemos en la imagen. Estos routers 2801 están configurados con HSRP¹¹, para en caso de caída de uno de ellos el otro coja el control y siga funcionando la red.

Antes de llegar a estos switches los paquetes pasan por los firewall ASA. Todo el tráfico que entra y sale de la sede central antes pasa por los firewall ASA 5520 dispuesto en modo failover¹², para controlar el tráfico que entra y sale de la red.

Una vez el paquete pasa por los switches MacroLan éste es transportado a través de la red MacroLan de telefónica hacia su destino gracias a las rutas configuradas en los switches antes mencionados.

La red MacroLan es una red conectada por fibra óptica con las sedes. El transporte se realiza a través de MPLS¹³.

¹¹ Hot Standby Router Protocol es un protocolo propiedad de CISCO que permite el despliegue de routers redundantes tolerantes a fallos en una red.

El funcionamiento del protocolo HSRP es el siguiente: Se crea un grupo (también conocido por el término inglés Clúster) de routers en el que uno de ellos actúa como maestro, enrutando el tráfico, y los demás actúan como respaldo a la espera de que se produzca un fallo en el maestro. HSRP es un protocolo que actúa en la capa 3 del modelo OSI administrando las direcciones virtuales que identifican al router que actúa como maestro en un momento dado.

¹² Failover, en español, tolerancia a fallos, es la capacidad de tener dos sistemas conectados idénticos para así en caso de que uno falle el otro se ponga operativo y todo siga funcionando.

Una vez llega a la sede los router VPNIP de telefónica enrutan el paquete hacia los Gateways de Cisco. Estos gateways son los que nos harían de Call Manager si fallan los dos Call Manager centrales a la vez y nos permitirían recibir y realizar llamadas como hemos explicado anteriormente. Estos gateways también nos permiten, a través de una conexión 3G, seguir enviando datos y llamadas a la sede central si las comunicaciones por MetroLan no están operativas. En ese caso el tráfico llegaría a la sede central a través del router 3G que vemos en la figura anterior.

Todo el tráfico que entra y sale de la sede central antes pasa por los firewall ASA 5520 dispuesto en modo failover, para controlar el tráfico que entra y sale de la red.

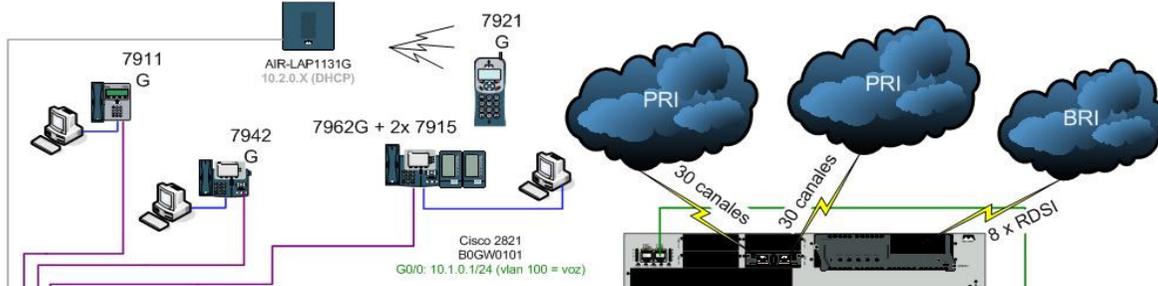
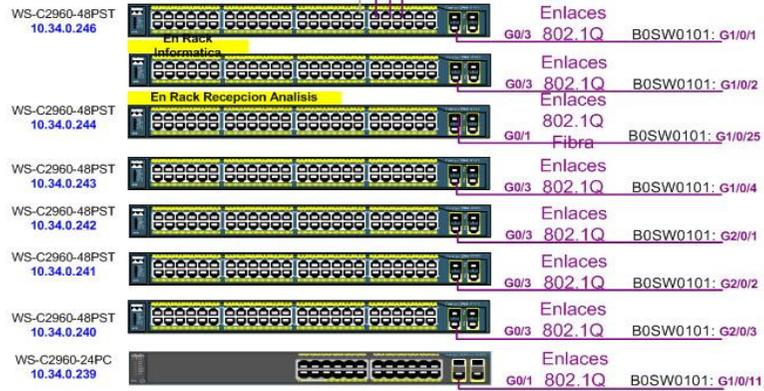
¹³ MPLS (Multiprotocol Label Switching), asigna a los datagramas de cada flujo una etiqueta única que permite una conmutación rápida en los routers intermedios (solo se mira la etiqueta, no la dirección de destino). Las principales aplicaciones de MPLS son:

- Funciones de ingeniería de tráfico (a los flujos de cada usuario se les asocia una etiqueta diferente)
- Policy Routing
- Servicios de VPN
- Servicios que requieren QoS
- MPLS se basa en el etiquetado de los paquetes en base a criterios de prioridad y/o calidad (QoS).

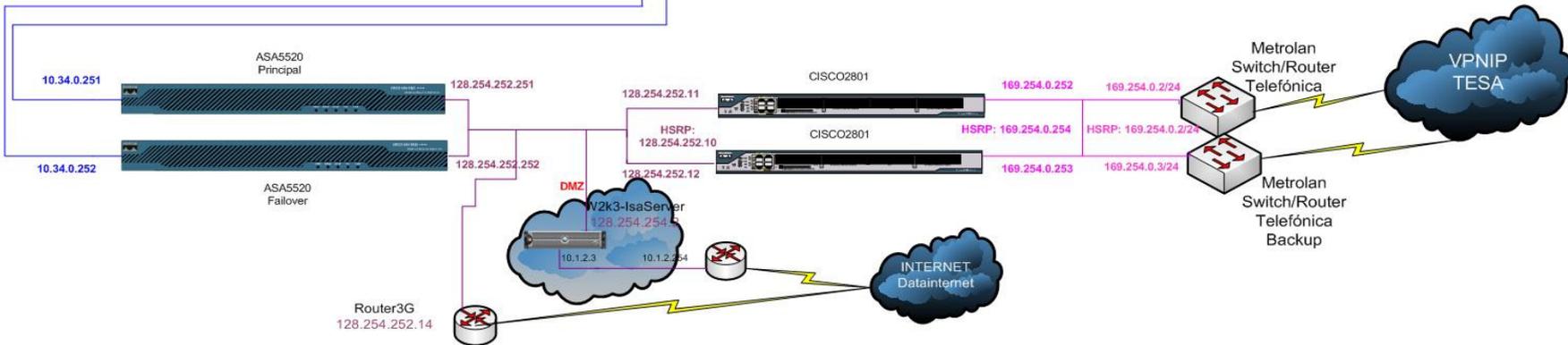
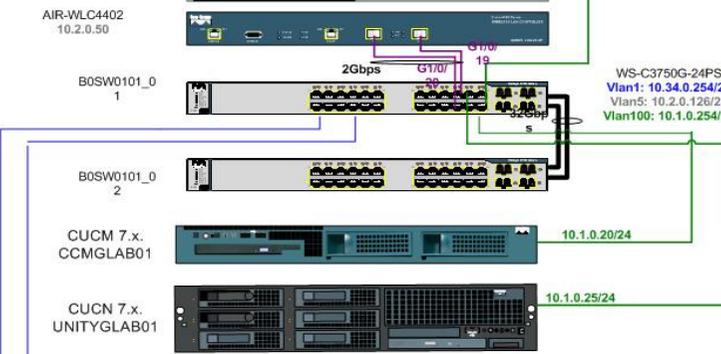
La idea de MPLS es realizar la conmutación de los paquetes o datagramas en función de las etiquetas añadidas en capa 2 y etiquetar dichos paquetes según la clasificación establecida por la QoS en la SLA. Por tanto MPLS es una tecnología que permite ofrecer QoS, independientemente de la red sobre la que se implemente. El etiquetado en capa 2 permite ofrecer servicio multiprotocolo y ser portable sobre multitud de tecnologías de capa de enlace: ATM, Frame Relay, líneas dedicadas, LANs.

Sede central

Descripcio	LAN	Red IP
Default	1	10.34.0.0/24
ap	5	10.2.0.0/25
voz	100	10.1.0.0/24
vpnip	25	169.254.0.0/24
invitados	200	10.2.0.128/25
Internet	300	x.x.x.x/y.y.y



- PRI
- 933636068
- 933636001
- 933636003
- 933636005
- 933636006
- 933636009
- 933636010
- 933636011
- 933636012
- 933636015
- 93363600.
- 93363601.
- 934053555



En el gráfico anterior podemos ver el esquema de comunicaciones de la sede central de Labco.

Podemos apreciar que hay dos puntos de entrada/salida de la red.

La primera es la VPNIP, por aquí saldrá y entrará todo el tráfico interno de la compañía hacia todas las demás sedes del grupo, tanto datos como las llamadas a extensiones. Como hemos explicado anteriormente hay dos switches que enrutan los paquetes conectados en HRSP para en caso de fallo de uno de ellos pueda seguir trabajando todo el grupo.

Las rutas de nuestros centros están configuradas en los Cisco 2801 de la imagen, para así poder configurar a donde queremos llegar desde la sede central.

Por último, una vez un paquete va a entrar en la red interna antes tiene que pasar por los routers ASA dispuestos en modo failover como anteriormente hemos explicado.

La otra entrada/salida de datos es la de Internet, todos los datos que tengan que ir a Internet, ftp con centros externos de la empresa, navegación de Internet y conexión con proveedores de la empresa saldrá por este punto. Antes de salir o entrar el tráfico a Internet, pasa por un servidor ISA Server¹⁴ para asegurar lo que entra en la red.

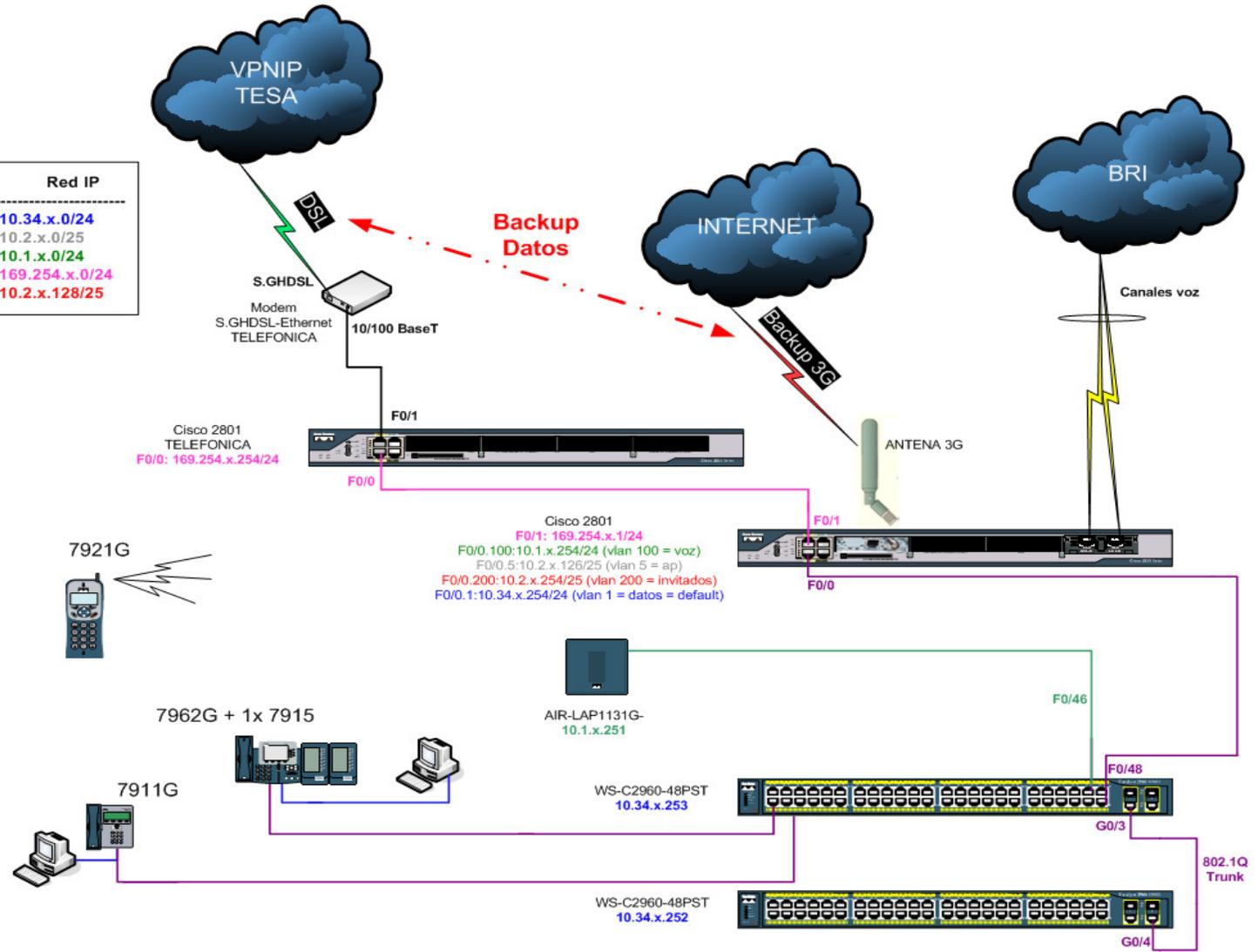
De Internet también vendrá el tráfico de otras sedes cuando haya fallado la conexión con la MacroLan y tenga que ponerse en marcha el backup de datos a través de 3G. Éste tráfico viene a través de un túnel VPN.

Una vez el tráfico a pasado los ASA éste se distribuye a través de los switches de nivel 3. En estos switches se conectan los Call Manager, los Unity, el wireles controler y todos los switches de nivel 2. En estos switches de nivel dos irán conectados todos los teléfonos, ordenadores y antenas de la sede.

¹⁴ Microsoft Internet Security and Acceleration Server (ISA Server) es un firewall de stateful packet inspection (es decir, analiza el encabezado de los paquetes IP) y de application layer (analizan la trama de datos en busca de tráfico sospechoso). Adicionalmente, ISA Server es un firewall de red, VPN y web cache.

Sede VPNIP

Descripcion	VLAN	Red IP
Default	1	10.34.x.0/24
ap	5	10.2.x.0/25
voz	100	10.1.x.0/24
vpnip	25	169.254.x.0/24
invitados	200	10.2.x.128/25



Cisco 2801 TELEFONICA
F0/0: 169.254.x.254/24

Cisco 2801
F0/1: 169.254.x.1/24
F0/0.100:10.1.x.254/24 (vlan 100 = voz)
F0/0.5:10.2.x.126/25 (vlan 5 = ap)
F0/0.200:10.2.x.254/25 (vlan 200 = invitados)
F0/0.1:10.34.x.254/24 (vlan 1 = datos = default)

AIR-LAP1131G-
10.1.x.251

WS-C2960-48PST
10.34.x.253

WS-C2960-48PST
10.34.x.252

802.1Q Trunk

En el gráfico anterior vemos la estructura interna de comunicaciones de una sede VPNIP, es decir, cualquier sede que no sea la central.

Vemos que todos los teléfonos van conectados a los switches configurables que hay en la sede. Según el centro habrá más o menos switches para conectar equipos. Los ordenadores se conectan a los teléfonos para conseguir IP o sino tienen teléfono directamente a los switches también.

Las antenas que nos proporcionan telefonía a los teléfonos inalámbricos, llamadas AIR-LAP1131G en el gráfico, también se conectan al switch con la interfaz configurada para la VLAN 100.

Los switches, para poder pasar tráfico entre ellos se conectan por un puerto configurado en modo DTP¹⁵ a velocidad de gigabit y éstos a la vez, al gateway Cisco 2801 también por una interfaz DTP a gigabit.

En este Gateway Cisco 2801 es donde está configurada la conexión 3G en caso de fallo en la conexión con MacroLan. En este Gateway también se conectan las conexiones de acceso básico (BRI). Estas conexiones son las que nos dan salida con número de teléfono analógico.

¹⁵ DTP (Dynamic Trunking Protocol) es un protocolo propietario creado por Cisco Systems que opera entre switches Cisco, el cual automatiza la configuración de trunking (etiquetado de tramas de diferentes VLAN's) en enlaces Ethernet.

3.4 Configuración básica de Cisco Unified Communications Manager

En esta sección explicaremos como hacer las configuraciones básicas de los Call Manager. Los Call Managers están configurados en cluster, por lo que toda configuración aplicada en el Call Manager central se verá aplicada en el de backup, para de este modo en caso de caída del principal la configuración del secundario sea exactamente la misma y no haya problemas con los teléfonos.

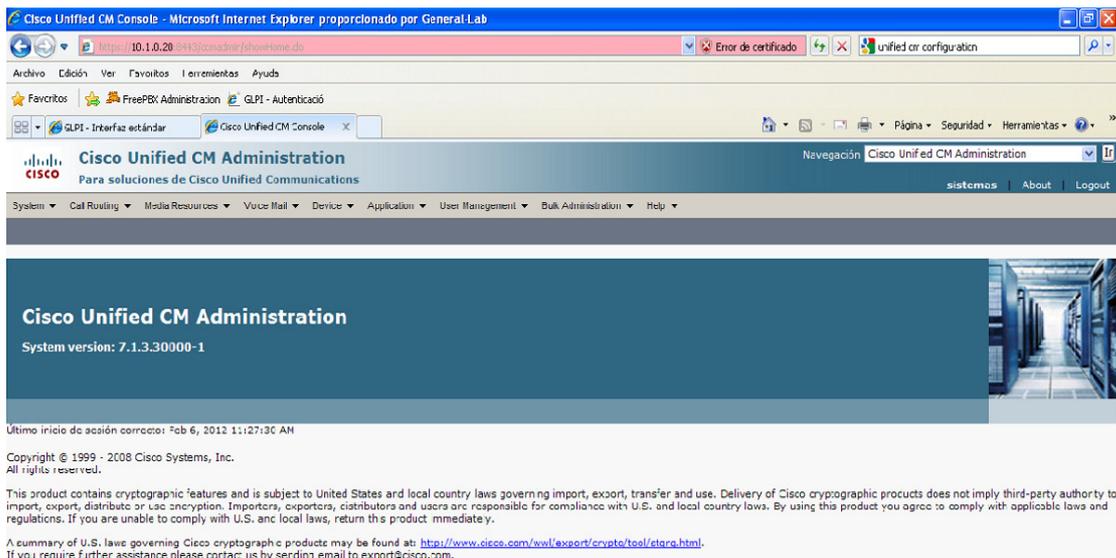
3.4.1 Introducción

El sistema Cisco Unified Communications Manager proporciona las funcionalidades de telefonía IP como pueden ser los teléfonos IP, gateways y aplicaciones multimedia así como servicios adicionales de voz, datos y videos como mensajes, conferencias.

Los Cisco Call Manager proporcionan además los servicios de señal y control de llamadas. Las funciones principales son:

- Proceso de llamadas
- Señales y control de dispositivos
- Administración del plan de marcación
- Administración de las características de los teléfonos
- Creación y mantenimiento del directorio telefónico
- Operaciones, administración, mantenimiento y aprovisionamiento

Para poder administrar el Call Manager tenemos que abrir un explorador y a través de la ip 10.1.0.20 ya nos pide usuario y contraseña. Una vez introducidos dichos parámetros ya entramos en la pantalla de administración y configuración de toda la centralita.



Una vez aquí vemos que tenemos diversos menús principales:

- Sistema
- Enrutamiento de llamadas
- Recursos de comunicación
- Correo de voz
- Dispositivo
- Aplicación
- Gestión de usuarios
- Administración de listas
- Ayuda

3.4.2 Administración del sistema (System)

En este menú configuraremos los parámetros básicos de configuración de la centralita, tales como la dirección IP, la referencia NTP, fecha y hora, los grupos de dispositivos y servicio de supervivencia en caso de fallo en los Call Managers.

3.4.2.1 Configuración de la IP del servidor

Para configurar la dirección IP del Call Manager:

System > Server y click **Add New**

Una vez allí nos encontramos la siguiente pantalla:

Cisco Unified CM Administration
Para soluciones de Cisco Unified Communications

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Server Configuration

Save

Status

Status: Ready

Server Information

Host Name/IP Address*

IPv6 Name

MAC Address

Description

*- indicates required item.

Tan solo hay que configurar la IP del servidor y la MAC de dicho servidor para poder asignar la IP a es MAC. Si queremos lo podemos poner una descripción.

En nuestro caso la configuración queda:

Cisco Unified CM Administration
Para soluciones de Cisco Unified Communications

Navegación Cisco Unified CM Adr

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Find and List Servers

Add New

Status

2 records found

Servers (1 - 2 de 2)

Buscar Servers donde

<input type="checkbox"/>	Host Name/IP Address ^	Description
<input type="checkbox"/>	10.1.0.20	CCMLAB01 Pub
<input type="checkbox"/>	10.1.85.20	CCMGLAB02 Sub

El primer servidor es el principal ubicado en Barcelona y el segundo es el de backup ubicado en Madrid, con ambos servidores conectados tenemos configurado un cluster.

Una vez definida la IP iremos a la configurar los puertos del cluster, para ello vamos a **Server > Cisco Unified CM**

The screenshot shows the Cisco Unified CM Administration interface. At the top, there is a navigation menu with options like System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. Below the navigation menu, the page title is 'Find and List Cisco Unified CMs'. A status bar indicates '2 records found'. Below this, there is a search bar with the text 'Buscar Cisco Unified Communications Managers donde' and a dropdown menu for 'empiece(n) por'. A table with two columns, 'Name' and 'Description', lists two records: 'CM_CCMGLAB01' with description 'CCMGLAB01' and 'CM_CCMGLAB02' with description 'CCMGLAB02'.

Vemos que tenemos ambas centralitas del cluster, si clickamos en una de ellas, vemos que podemos configurar la descripción de cada una y los puertos que utilizan, en nuestro caso quedan ambas de la siguiente forma:

The screenshot shows the Cisco Unified CM Administration interface for configuring a Cisco Unified Communications Manager. The page title is 'Cisco Unified CM Configuration'. Below the title, there are buttons for 'Save', 'Reset', and 'Apply Config'. A status bar indicates 'Status: Ready'. Below this, there is a section for 'Cisco Unified Communications Manager Information' with the text 'Cisco Unified Communications Manager: CM_CCMGLAB01 (used by 839 devices)'. Below this, there is a section for 'Server Information' with fields for 'CTI ID' (1), 'Cisco Unified Communications Manager Server*' (10.1.0.20), 'Cisco Unified Communications Manager Name*' (CM_CCMGLAB01), and 'Description' (CCMGLAB01). Below this, there is a section for 'Auto-registration Information' with fields for 'Starting Directory Number*' (1000), 'Ending Directory Number*' (1000), 'Partition' (< None >), and 'External Phone Number Mask'. A checkbox for 'Auto-registration Disabled on this Cisco Unified Communications Manager' is checked. Below this, there is a section for 'Cisco Unified Communications Manager TCP Port Settings for this Server' with fields for 'Ethernet Phone Port*' (2000), 'MGCP Listen Port*' (2427), 'MGCP Keep-alive Port*' (2428), 'SIP Phone Port*' (5060), and 'SIP Phone Secure Port*' (5061). At the bottom, there are buttons for 'Save', 'Reset', and 'Apply Config'. A note at the bottom indicates '*- indicates required item.'

Los parámetros de **Auto-registration Information** nos permiten configurar, en caso de querer que al conectar un dispositivo se nos asigne una extensión automática, el número de extensión que queremos que empiece a asignarse y el número de extensión final. En

nuestro caso esto no nos interesa y tenemos chequeada la opción de tener esta opción deshabilitada.

3.4.2.2 Configuración de la referencia NTP

NTP (Network Time Protocol) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del ruteo de paquetes en redes con latencia variable.

En nuestro caso cogemos como referencia NTP los servidores NTP configurados en el Gateway instalado en la sede central con IP 10.1.0.1.

Para configurar los servidores NTP primero tenemos que elegir qué servidores queremos usar para ello y conocer su IP pública. Cuando ya sepamos esto, abrimos una consola:

```
telnet 10.1.0.1
```

```
B0GW0101#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
B0GW0101(config)# ntp server 129.69.1.153 prefer
```

```
B0GW0101(config)# ntp server 192.5.41.209
```

```
B0GW0101(config)# ntp server 130.159.196.118
```

Podemos ver que hemos configurado tres por si acaso falla alguno pero hemos puesto el 129.69.1.153 por defecto

Ahora si ejecutamos el comando **show-running-config**, al final de la configuración nos aseguramos que tenemos los NTP en el sistema.

```
ntp server 129.69.1.153 prefer
ntp server 192.5.41.209
ntp server 130.159.196.118
end
```

Para crear el NTP vamos a **System > Phone NTP Reference > Add New**. Una vez allí tan solo tenemos que poner la IP 10.1.0.1 para que nos coja ese Gateway como servidor de hora, la descripción y el modo en que se enviarán los paquetes NTP.

The screenshot displays the Cisco Unified CM Administration web interface. At the top, the Cisco logo and the text "Cisco Unified CM Administration" are visible, along with the tagline "Para soluciones de Cisco Unified Communications". Below this is a navigation menu with items: System, Call Routing, Media Resources, Voice Mail, Device, Application, and User Management. The main heading is "Phone NTP Reference Configuration". Below the heading are three buttons: "Save" (with a floppy disk icon), "Delete" (with a red X icon), and "Add New" (with a plus icon). A "Status" section shows an information icon and the text "Status: Ready". The "Phone NTP Reference Information" section contains three input fields: "IP Address*" with the value "10.1.0.1", "Description" with the value "GW Voz Londres 28", and "Mode*" with a dropdown menu set to "Unicast". Below these fields are three buttons: "Save", "Delete", and "Add New". At the bottom, there is an information icon and the text "*- indicates required item."

3.4.2.3 Configuración de fecha y hora

Configuraremos un grupo de fecha/hora para la configuración de los dispositivos que se encuentran en la península y otro para la configuración de los dispositivos que se encuentran en las islas Canarias.

Para configurarlo vamos a **System > Date/Time Group > Add New.**

Una vez aquí configuramos el nombre del grupo que queremos darle, la zona horaria en la que se encuentra el grupo, el separador que queremos en el formato de la fecha, el formato de la fecha y si queremos el formato de la hora en 24 horas o en formato 12 horas.

Por último tenemos que añadir todas las referencias NTP que queremos que tenga el grupo. En nuestro caso ambos el grupo de la península queda:

The screenshot shows the Cisco Unified CM Administration interface for the 'Date/Time Group Configuration' of the 'CMLocal' group. The status is 'Ready'. The configuration details are as follows:

- Date/Time Group Information:**
 - Date/Time Group: CMLocal (used by 824 devices)
 - Group Name*: CMLocal
 - Time Zone*: (GMT+1:00) Europe/Prague* (Entries with * are compatible with legacy phone loads)
 - Separator*: / (slash) (applies to Date Format only)
 - Date Format*: D/M/Y
 - Time Format*: 24-hour
- Phone NTP References for this Date/Time Group:**
 - Selected Phone NTP References**: 10.1.0.1
 - Buttons: Add Phone NTP References, Remove Phone NTP References

At the bottom, there are control buttons: Save, Delete, Copy, Reset, Apply Config, and Add New. A legend indicates that '*' indicates a required item and '**Selected Phone NTP References are ordered by highest priority'.

Y la configuración de Canarias:

The screenshot shows the Cisco Unified CM Administration interface for the 'Date/Time Group Configuration' of the 'Canarias' group. The status is 'Ready'. The configuration details are as follows:

- Date/Time Group Information:**
 - Date/Time Group: Canarias (used by 15 devices)
 - Group Name*: Canarias
 - Time Zone*: (GMT) Etc/GMT* (Entries with * are compatible with legacy phone loads)
 - Separator*: / (slash) (applies to Date Format only)
 - Date Format*: D/M/Y
 - Time Format*: 24-hour
- Phone NTP References for this Date/Time Group:**
 - Selected Phone NTP References**: 10.1.0.1
 - Buttons: Add Phone NTP References, Remove Phone NTP References

At the bottom, there are control buttons: Save, Delete, Copy, Reset, Apply Config, and Add New. A legend indicates that '*' indicates a required item and '**Selected Phone NTP References are ordered by highest priority'.

3.4.2.4 Configuración del SRST

SRST (Survivable Remote Site Telephony) se utiliza para detectar automáticamente un fallo en la red e iniciar un proceso de configuración automática en el Gateway del centro remoto, proporcionando el procesamiento de llamadas, de copia de seguridad para los teléfonos IP de esa oficina y ayudar a asegurar que las capacidades de telefonía se mantengan en funcionamiento. Tras la restauración de la conectividad WAN, el sistema cambia automáticamente el procesamiento de llamadas de nuevo al Cisco Call Manager principal. La configuración de Cisco Unified SRST debe ser completada sólo una vez, durante la instalación, simplifica la implementación, administración y mantenimiento.

Para configurar la SRST de cada centro vamos a **System > SRST > Add New**. Debemos configurar tantos SRSTs como Gateways tengamos en centros remotos.

En nuestro caso tenemos la siguiente lista:

Cisco Unified CM Administration			
Para soluciones de Cisco Unified Communications			Navegación Cisco Unified
System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾			
Find and List SRST References			
<input type="button" value="Add New"/> <input type="button" value="Select All"/> <input type="button" value="Clear All"/> <input type="button" value="Delete Selected"/> <input type="button" value="Reset Selected"/> <input type="button" value="Apply Config to Selected"/>			
<input type="checkbox"/>	Name ^	IP Address	SCCP Port
<input type="checkbox"/>	AL67GW0101	10.1.67.1	2000
<input type="checkbox"/>	AL147GW0101	10.1.47.1	2000
<input type="checkbox"/>	B12GW101	10.1.12.1	2000
<input type="checkbox"/>	B13GW0101	10.1.13.1	2000
<input type="checkbox"/>	B13GW101	10.1.13.1	2000
<input type="checkbox"/>	B17GW101	10.1.17.1	2000
<input type="checkbox"/>	B18GW0101	10.1.18.1	2000
<input type="checkbox"/>	B18GW101	10.1.18.1	2000
<input type="checkbox"/>	B20GW0101	10.1.20.1	2000
<input type="checkbox"/>	B20GW101	10.1.20.1	2000
<input type="checkbox"/>	B21GW101	10.1.21.1	2000
<input type="checkbox"/>	B22GW101	10.1.22.1	2000
<input type="checkbox"/>	B24GW0101	10.1.24.1	2000
<input type="checkbox"/>	B26GW101	10.1.26.1	2000
<input type="checkbox"/>	B32GW0101	10.1.32.1	2000
<input type="checkbox"/>	B55GW0101	10.1.55.1	2000
<input type="checkbox"/>	B57GW0101	10.1.57.1	2000
<input type="checkbox"/>	B59GW0101	10.1.59.1	2000
<input type="checkbox"/>	BAD77GW0101	10.1.77.1	2000
<input type="checkbox"/>	C23GW101	10.1.23.1	2000
<input type="checkbox"/>	COR40GW0101	10.1.40.1	2000
<input type="checkbox"/>	GE48GW0101	10.1.48.1	2000
<input type="checkbox"/>	GE49GW0101	10.1.49.1	2000
<input type="checkbox"/>	GE56GW0101	10.1.56.1	2000
<input type="checkbox"/>	ICA39GW0101	10.1.39.1	2000
<input type="checkbox"/>	LER58GW0101	10.1.58.1	2000
<input type="checkbox"/>	M27GW0101	10.1.27.1	2000
<input type="checkbox"/>	M28GW0101	10.1.28.254	2000
<input type="checkbox"/>	M29GW0101	10.1.29.1	2000
<input type="checkbox"/>	M30GW0101	10.1.30.1	2000
<input type="checkbox"/>	M31GW0101	10.1.31.1	2000
<input type="checkbox"/>	M60GW0101	10.1.60.1	2000
<input type="checkbox"/>	M62GW0101	10.1.62.1	2000
<input type="checkbox"/>	M63GW0101	10.1.63.1	2000
<input type="checkbox"/>	M64GW0101	10.1.64.1	2000
<input type="checkbox"/>	M65GW0101	10.1.65.1	2000
<input type="checkbox"/>	M68GW0101	10.1.68.1	2000
<input type="checkbox"/>	M85GW0101	10.1.85.1	2000
<input type="checkbox"/>	M89GW0101	10.1.89.1	2000
<input type="checkbox"/>	MA15GW0101	10.1.15.1	2000
<input type="checkbox"/>	MA16GW0101	10.1.16.1	2000
<input type="checkbox"/>	MA71GW0101	10.1.71.1	2000
<input type="checkbox"/>	MAN14GW0101	10.1.14.1	2000
<input type="checkbox"/>	MAN54GW0101	10.1.54.1	2000
<input type="checkbox"/>	MAR35GW0101	10.1.35.1	2000
<input type="checkbox"/>	MU51GW0101	10.1.51.1	2000
<input type="checkbox"/>	PM37GW0101	10.1.37.1	2000
<input type="checkbox"/>	PM69GW0101	10.1.69.1	2000
<input type="checkbox"/>	PM70GW0101	10.1.70.1	2000
<input type="checkbox"/>	S41GW0101	10.1.41.1	2000

Para ver un ejemplo el SRST de la sede de Hospital Xanit en Málaga queda:

The screenshot displays a configuration page for SRST. It is divided into three main sections:

- Status:** Shows an information icon and the text "Status: Ready".
- SRST Reference Status:** Shows "SRST Reference: MA15GW0101 (used by 7 devices)".
- SRST Reference Information:** A form with the following fields:
 - Name*: MA15GW0101
 - Port*: 2000
 - IP Address*: 10.1.15.1
 - SIP Network/IP Address: (empty)
 - SIP Port*: 5060
 - SRST Certificate Provider Port*: 2445
 - Is SRST Secure?:

At the bottom, there are buttons for "Save", "Delete", "Copy", "Reset", "Apply Config", and "Add New". Below the buttons is an information icon and the text "*- indicates required item."

En la primera sección vemos el estado de la conexión y nos indica que tiene 7 dispositivos activos.

En la sección siguiente es donde se realiza la conexión. Le damos un nombre al SRST, el puerto por donde se comunica, la dirección IP del Gateway que tiene el SRST y el puerto SIP que por defecto es 5060.

3.4.2.5 Configuración de las Device Pool

En la Device Pool definimos las características comunes para los dispositivos, aunque contiene sólo la información del dispositivo y la ubicación relacionada.

Tenemos que asegurarnos que cada dispositivo está asociado con un conjunto de dispositivos y con una configuración del dispositivo común. Haremos una Device Pool para cada centro.

Para configurarlas vamos a **System > Device Pool > Add New**. Una vez allí tendremos que configurar los siguientes parámetros:

- **Device Pool Name:** el nombre de la Device Pool

- **Cisco Unified Communications Manager Group:** especifica una lista priorizada de Call Managers administrativos. El primero en la lista es el principal para ese grupo, y los demás miembros del grupo sirven como backup en caso de caída del principal.
- **Local Route Group:** con este parámetro simplemente configuramos por que Gateway queremos que salgan las llamadas. En el desplegable tenemos que seleccionar el Route Group que hayamos configurados para esa sede.

Para configurar el route Group vamos a **Call Routing > Route/Hunt > Route Group > Add New**. Una vez allí tan solo tenemos que darle nombre a la ruta, ponemos al Algoritmo de Distribución circular aunque este parámetro no importa porque solo tendremos un Gateway asociado, y agregamos la IP del Gateway del centro donde nos encontramos. En el caso del Hospital de Xanit queda:

The screenshot displays the configuration page for a new Route Group. It is divided into three main sections:

- Route Group Information:** Contains fields for 'Route Group Name*' (RG_MA15_Xanit) and 'Distribution Algorithm*' (Circular).
- Route Group Member Information:** Includes a 'Find Devices to Add to Route Group' section with a search box and a 'Find' button. Below it, a list of 'Available Devices**' is shown, with 10.1.0.1 selected. Other devices listed are 10.1.12.1, 10.1.13.1, 10.1.14.1, and 10.1.15.1. A 'Port(s)' dropdown is set to 'All'. An 'Add to Route Group' button is present.
- Current Route Group Members:** Shows 'Selected Devices***' as '10.1.15.1 (All Ports)'. There is a 'Reverse Order of Selected Devices' button and a 'Removed Devices****' section.

- **Date/Time Group:** seleccionamos el grupo de la Península o de Canarias según donde este situado el centro.
- **Region:** la configuración Region especifica el codec de voz que puede ser usado para llamadas dentro de una región y entre otras regiones. Elegimos para cada centro su Region configurada.

- **Media Resource Group List:** esta opción proporciona un mecanismo para la gestión de recursos de los medios, por lo que todos los Call Managers de Cisco dentro de un grupo puede compartir. Recursos de los medios de comunicación ofrecen conferencias, transcodificación, la terminación medios de comunicación, anunciador, y la música en las bodegas de los servicios.
- **SRST Reference:** esta opción hemos explicado anteriormente lo que era y como configurarla. También escogeremos el SRST que hemos configurado para el centro que estamos configurando.

Por tanto la configuración de Device Pool para Hospital Xanit queda:

The screenshot displays the Cisco Unified CM Administration web interface for configuring a Device Pool. The page title is "Cisco Unified CM Administration" with the subtitle "Para soluciones de Cisco Unified Communications". The navigation menu includes System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help.

The main section is "Device Pool Configuration" for the device pool "DP_MA15_Xanit (10 members**)". The status is "Ready".

Device Pool Settings:

Device Pool Name*	DP_MA15_Xanit
Cisco Unified Communications Manager Group*	CMG_GLABSUBPUB
Calling Search Space for Auto-registration	< None >
Reverted Call Focus Priority	Predeterminado
Local Route Group	RG_MA15_Xanit

Roaming Sensitive Settings:

Date/Time Group*	CMLocal
Region*	MA15
Media Resource Group List	MRGL_SUBPUB
Location	Hub_None
Network Locale	España
SRST Reference*	MA15GW0101
Connection Monitor Duration***	
Single Button Barge*	Predeterminado
Join Across Lines*	Predeterminado
Physical Location	< None >
Device Mobility Group	< None >

3.4.3 Configuración de extensiones

Para configurar extensiones en el Call Manager tenemos que dar de alta primero el dispositivo por su MAC y después asignar esa MAC a una extensión.

3.4.3.1 Configuración del teléfono

Para dar de alta un dispositivo vamos a **Device > Phone > Add New**.

Lo primero que nos encontramos es la siguiente pantalla en la que tenemos que elegir el teléfono que vamos a configurar para que cuando conectemos el teléfono a la red el Call Manager le pase el firmware de su modelo y se configure correctamente.

En la siguiente pantalla elegimos el protocolo SCCP, el protocolo de señal de Cisco, ya que estamos utilizando teléfonos de Cisco.

Una vez hecho esto tenemos que configurar:

- **MAC Adress:** introducimos la dirección MAC del dispositivo que estamos configurando.
- **Description:** elegimos la descripción del teléfono, normalmente pondremos el nombre de la extensión que le asignaremos más tarde.

- **Device Pool:** elegimos la Device Pool del centro en el que estará el teléfono.
- **Phone Button Template:** esta opción determina la configuración de los botones y que características tiene cada botón. En este desplegable normalmente solo tendremos una opción a elegir.
- **Calling Search Space:** elegiremos el Calling Search Space adecuado a la extensión. Con el Calling Search Space podemos elegir las restricciones de cada extensión a llamar a determinadas extensiones o números externos, como puede ser controlar que no se permita llamar a móviles o al extranjero.
- **User Locale:** elegimos España, para que el idioma del dispositivo nos lo configure en español.

Si hemos configurado todo bien al conectar el teléfono a la red veremos como empieza a actualizar el firmware. Pero ahora falta asignarle una extensión al teléfono para poder llamar y un nombre de usuario para poder encontrar a la persona por el directorio corporativo del teléfono y que salga el nombre cuando se llama.

3.4.3.2 Configuración de la extensión

Una vez hayamos configurado el teléfono y este conectado vemos al principio de la descripción que esta registrado en el Call Manager 10.1.0.20 y que se le ha asignado la IP 10.1.21.187 y también vemos dos OKs conforme esta activo y conectado.

Si nos fijamos a la izquierda vemos “Line [1] – Add a new DN” y “Line [2] – Add a new DN”, por lo que tenemos que asignar una línea a dicho dispositivo para poder utilizarlo.

Status
 Status: Ready

Association Information
 Modify Button Items

1	Line [1] - Add a new DN
2	Line [2] - Add a new DN
3	Add a new SD
4	Add a new SD
5	Add a new SD
6	Add a new SD
----- Unassigned Associated Items -----	
7	Add a new URL
8	Add a new SURL
9	Add a new BLF Directed Call Park
10	No molestar
11	Intercom [1] - Add a new Intercom
12	Movilidad
13	Add a new BLF SD
14	Privado
15	Ninguno

Phone Type
 Product Type: Cisco 7921
 Device Protocol: SCCP

Device Information

Registration	Registered with Cisco Unified Communications Manager 10.1.0.20
IPv4 Address	10.1.21.187
Active Load ID	Unknown
<input checked="" type="checkbox"/> Device is Active	
<input checked="" type="checkbox"/> Device is trusted	
MAC Address*	001BD458E8A2
Description	Prueba
Device Pool*	DP_B0_Central View Details
Common Device Configuration	< None > View Details
Phone Button Template*	Standard 7921 SCCP
Softkey Template	Standard User 7921 Grupo GLAB
Common Phone Profile*	Standard Common Phone Profile
Calling Search Space	CSSTotal
AAR Calling Search Space	< None >
Media Resource Group List	< None >
User Hold MOH Audio Source	< None >
Network Hold MOH Audio Source	< None >
Location*	Hub_None
AAR Group	< None >
User Locale	Español, Reino de España
Network Locale	< None >
Built In Bridge*	Predeterminado

Para configurar una nueva extensión clickamos encima de “Line [1] – Add a new DN” y llegamos a la página de configuración de una extensión llamada **Directory Number Configuration**. Si más tarde queremos llegar a esta página para ver que extensiones estan configuradas solo hay que ir a **Call Routing > Directory Number** y buscar la que queramos o ver todas las que hay.

Cuando estamos en la página de configuración hay que configurar:

- **Directory Number:** el número que queremos que tenga la extensión.
- **Route Partition:** elegimos la partición a la que pertenecerá la extensión. Normalmente por defecto nuestras extensiones pertenecerán a la partición InternasGlab ya que son siempre extensiones internas.
- **Description:** descripción de la extensión
- **Alerting Name:** escribimos el nombre que queremos que le aparezca en pantalla a la persona que llama a esta extensión. Si dejamos esta opción en blanco entonces
- **ASCII Alerting Name:** es lo mismo que antes pero hay que limitar los caracteres a ASCII para los teléfonos que no soportan caracteres UNICODE.

- **Calling Search Space:** elegiremos el Calling Search Space que queramos, como hemos explicado antes según el que escojamos podremos llamar a uno o otros sitios o a todos los sitios.

Esta es la configuración básica de una extensión. Una vez configurada cuando le demos a **Save** el teléfono se reiniciará y cuando vuelva a iniciarse veremos que ya tiene la configuración que le hayamos configurado y en la página de Directory Number nos saldrá un cuadro con los dispositivos que tiene asociados dicha extensión:

Status

 Status: Ready

Directory Number Information

Directory Number*

Route Partition

Description

Alerting Name

ASCII Alerting Name

Allow Control of Device from CTI

Associated Devices

▼ ▲

Dissociate Devices

Directory Number Settings

Voice Mail Profile (Choose <None> to use system default)

Calling Search Space

Presence Group*

User Hold MOH Audio Source

Network Hold MOH Audio Source

Auto Answer*

3.4.3.3 Configuración del directorio (End User)

Para tener un directorio de todas las extensiones de Cisco, tenemos que añadir las extensiones que queramos que aparezcan en el teléfono cuando buscamos el directorio por el teléfono.

Para añadir una extensión al directorio vamos a **User Management > End User > End User**.

Una vez allí tenemos que configurar:

- **User ID:** el número de la extensión que queremos configurar en el directorio.
- **Last Name:** el nombre de la persona que tiene la extensión.
- **User Locale:** configuramos en español.
- Al final de la página de configuración en la sección **Permissions Information** clickamos en **Add to User Group** y metemos en la lista el grupo “Standard CCM End Users”.

Una vez hecho esto ya podremos ver la extensión en el directorio.

3.4.4 Enrutamiento de llamadas (Call Routing)

En esta sección configuraremos todo lo relativo al enrutamiento de llamadas y que comportamiento tienen que tener depende de donde llamemos. También configuraremos los permisos de llamadas tales como poder realizar llamadas internacionales o a móviles.

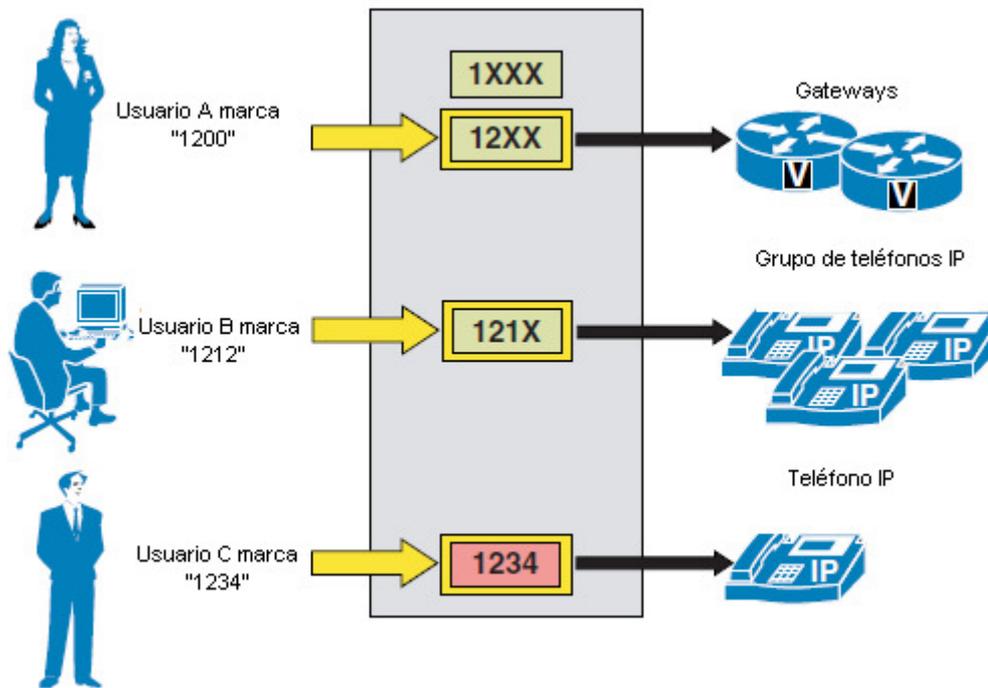
Todos los destinos de marcación configurados en el Call Manager se añaden tabla de enrutamiento interna de éste.

Estos destinos incluyen las líneas de telefonía IP, los puertos de correo de voz, patrones de rutas y patrones de traducción.

Cuando se marca un número, el Call Manager busca en su tabla de enrutamiento la coincidencia más cercana a ese número marcada. En la práctica, cuando hay varios patrones potencialmente coincidentes, el patrón de destino se elige sobre los siguientes criterios:

- Se ajusta a los dígitos marcados, y
- Entre todos los patrones potencialmente coincidentes, se escoge el que coincide con el menor número dígitos que no sean del número marcado.

Por ejemplo, consideremos el caso de la siguiente imagen, donde la tabla de encaminamiento de llamadas incluye los patrones 1xxx, 12xx y 1234.



Cuando el usuario A marca la extensión 1200, el Call Manager compara dicho número en su tabla de enrutamiento de llamadas. En este caso, hay dos posibles resultados, 1xxx y 12xx. Ambos coinciden con el marcado, pero 1xxx coincide con un total de 1.000 números (del 1000 al 1999), mientras que 12xx sólo coincide en 100 números (1200 a 1299). Por lo tanto, 12xx se selecciona como el destino de esta llamada.

Cuando el usuario B marca el número 1212, hay tres patrones potencialmente coincidentes, 1xxx, 12xx y 121x. Como hemos mencionado anteriormente, los números de marcación 1xxx coinciden en 1000 números y para 12xx coinciden con 100. Sin embargo, 121x coincide con solamente 10 números, por lo que se selecciona éste como destino de la llamada.

Cuando el usuario C marca 1234, hay tres patrones potencialmente compatibles 1xxx, 12xx, y 1234. Como hemos mencionado anteriormente, los patrones de 1xxx coinciden con 1000 números y 12xx coinciden con 100. Sin embargo, 1234 sólo coincide con una sola extensión (la misma que a marcado), por lo que se selecciona como el destino de esta llamada.

3.4.4.1 Reglas de marcación (Dial Rules)

En esta sección configuraremos el comportamiento de las llamadas que tienen que ir por PSTN¹⁶, es decir, cuando haya que llamar a números al exterior convencionales.

Para ello vamos a **Call Routing > Dial Rules > Application Dial Rules**. Configuraremos tres reglas de marcación para llamadas internacionales, llamadas nacionales y llamadas a móviles.

Para configurarlas clickamos en **Add New**. Una vez allí le damos nombre a la regla, una descripción, el dígito por el que empieza dicha regla y el número de dígitos que tendrán los números de marcación de dicha regla.

En el caso de marcación a móviles queda:

The screenshot displays the 'Application Dial Rule Configuration' page. At the top, there are navigation menus for System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. Below the navigation is a header bar with 'Application Dial Rule Configuration' and 'Related Links: Ba'. A toolbar contains 'Save', 'Delete', and 'Add New' buttons. The main content area is divided into sections: 'Status' (Ready), 'Application Dial Rule Information' (form fields for Name, Description, Number Begins With, Number of Digits, Total Digits to be Removed, and Prefix With Pattern), and 'Application Dial Rule Priority' (a table of existing rules). At the bottom, there are 'Save', 'Delete', and 'Add New' buttons.

Name	Number Begins With	Number of Digits	Total Digits to be Removed	Prefix With Pattern
Nacionales	9	9	0	0
Moviles	6	9	0	0
Internacionales00	00	14	0	0

En el caso de móviles vemos que los números empiezan por 6 y que tienen 9 dígitos. Tenemos que hacer lo mismo para las demás reglas.

Como podemos ver en la tabla de debajo de la imagen anterior vemos que las llamadas internacionales empiezan por 00 y tienen 14 dígitos en total y las llamadas nacionales empiezan por 9 y tienen 9 dígitos de longitud.

¹⁶ Public Switch Telephony Network, es la red de telefonía básica.

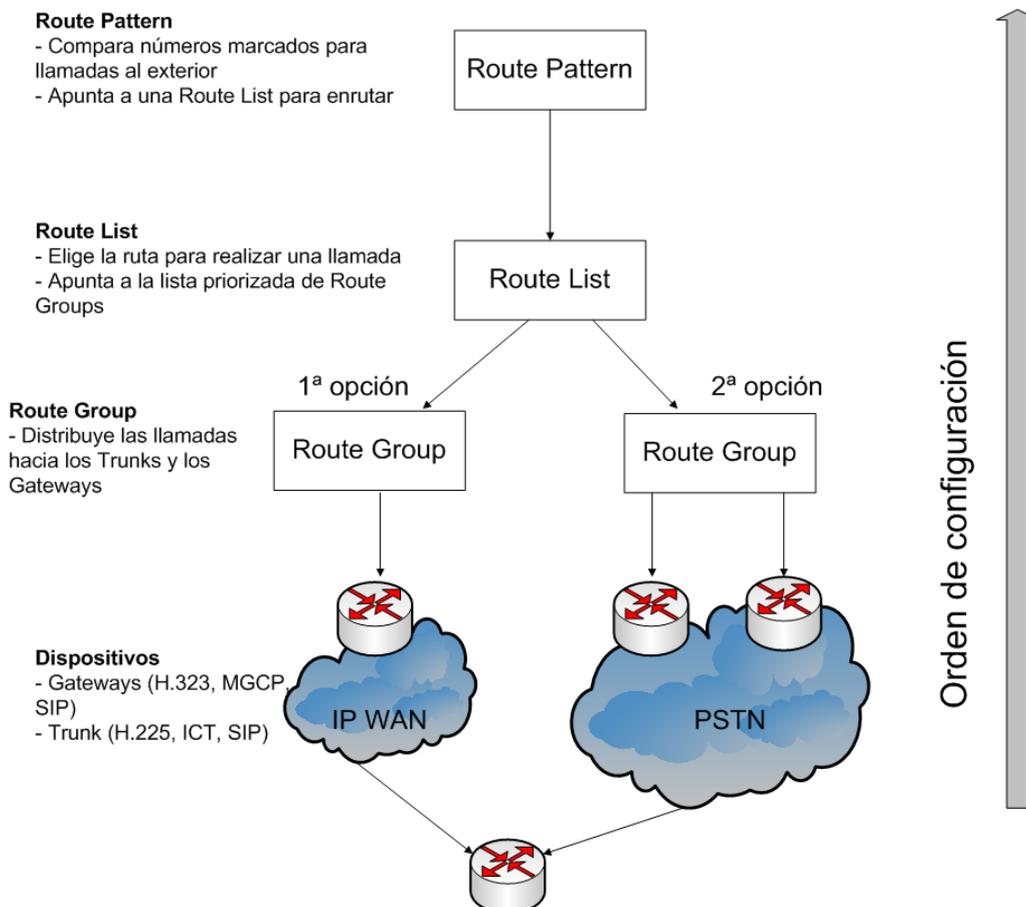
3.4.4.2 Configuración de marcaciones externas (Route/Hunt)

El Cisco Call Manager de forma automática sabe como enrutar las llamadas a extensiones internas.

Para los destinos externos que necesiten una ruta específica para llegar a realizarse la llamada, tales como las puertas de enlace PSTN, marcación de números convencionales, salidas para los datáfonos, salidas para móviles, etc.

Estas rutas se basan en la construcción de una arquitectura de tres niveles la cual permite múltiples capas de enrutamiento de llamada. El Call Manager compara el número marcado que tiene que ser enrutado hacia el exterior con un patrón de rutas ya configuradas y utiliza dicha patrón para seleccionar la lista de rutas, que es una lista priorizada de los caminos disponibles para realizar la llamada. Estos caminos son conocidos como grupos de rutas (Route Groups) y son similares a los grupos de trunks en la terminología tradicional PBX.

En la siguiente imagen vemos la arquitectura de tres niveles utilizada por el Call Manager para construir la ruta de las llamadas externas:



3.4.4.2.1 Route Group

Con los Route Group asignamos el orden en el que los trunks y los gateways son seleccionados, es decir, nos permite priorizar la lista de gateways y puertos trunk de salida.

Como hemos explicado en la sección anterior, en nuestro caso, configuraremos el Gateway que se encuentre en la sede para que salgan por allí las llamadas.

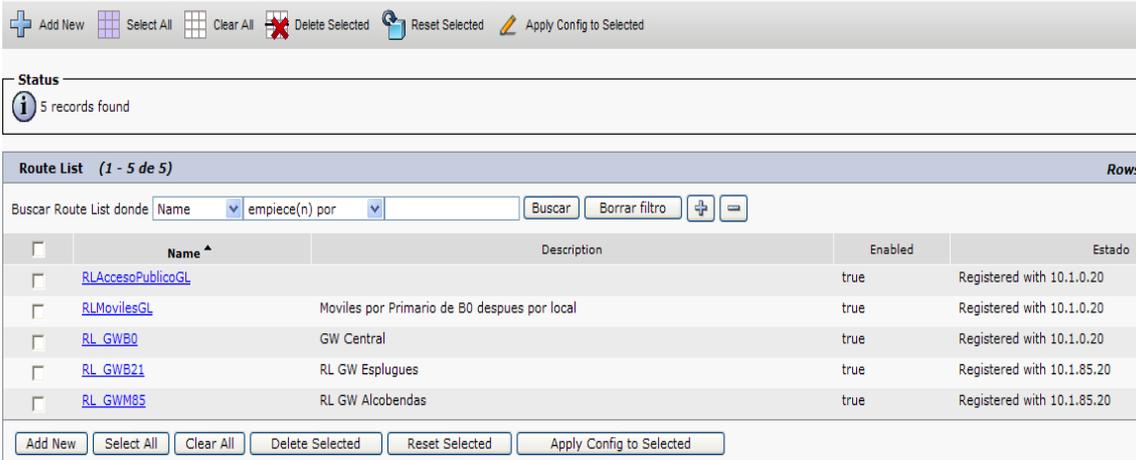
3.4.4.2.2 Route List

Es una lista priorizada de rutas para una llamada saliente. Un uso típico de una lista de rutas consiste en especificar dos caminos para un destino remoto, donde la primera elección es a través de la IP WAN y la segunda elección es a través de una puerta de enlace PSTN.

Las Route List tienen las siguientes características:

- Múltiples Route Patterns pueden apuntar a una misma Route List
- Una Route List es una lista priorizada de Route Groups que funcionan como caminos alternativos para un mismo destino.
- Múltiples Route List pueden permanecer al mismo Route Group.

Para configurar una Route List vamos a **Call Routing > Route/Hunt > Route Pattern > Add New**



The screenshot shows a web interface for configuring Route Lists. At the top, there are several action buttons: Add New, Select All, Clear All, Delete Selected, Reset Selected, and Apply Config to Selected. Below this is a status bar indicating "5 records found". The main area is a table titled "Route List (1 - 5 de 5)" with columns for Name, Description, Enabled, and Estado. The table contains five entries, each with a checkbox in the first column.

<input type="checkbox"/>	Name ^	Description	Enabled	Estado
<input type="checkbox"/>	RLAccesoPublicoGL		true	Registered with 10.1.0.20
<input type="checkbox"/>	RLMovilesGL	Moviles por Primario de B0 despues por local	true	Registered with 10.1.0.20
<input type="checkbox"/>	RL_GWB0	GW Central	true	Registered with 10.1.0.20
<input type="checkbox"/>	RL_GWB21	RL GW Esplugues	true	Registered with 10.1.85.20
<input type="checkbox"/>	RL_GWM85	RL GW Alcobendas	true	Registered with 10.1.85.20

At the bottom of the table, there are buttons for Add New, Select All, Clear All, Delete Selected, Reset Selected, and Apply Config to Selected.

Estos son los Route List que tenemos configurados. Tenemos para los móviles, para que salgan por el primario del Gateway de la sede central, por el de la sede de Esplugues,

por el de Madrid y por último tenemos el Route List de Acceso Público, que es el que asignaremos a las demás sedes. Esta Route List tiene como primera salida el Gateway local con lo que si la sede se encuentra en Málaga, al llamar a un número externo desde allí en el teléfono que recibe la llamada verá el prefijo 952, el de Málaga. Si no hiciéramos esto el usuario que recibe la llamada podría ver un 93 que es la salida de Barcelona. Este tipo de funcionalidad también la tenemos para la Route List de Móviles, para cuando la llamada sea a móvil es decir que el número empiece por 6. La diferencia es que para móviles como primera salida tenemos el primario de la sede central y en caso de fallo se saldría por el primario de la sede local.

Así pues, por ejemplo, la Route List RLAccesoPublicoGL esta configurada:

The screenshot shows the 'Route List Configuration' page. At the top, there is a navigation menu with options like System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. Below the menu, the page title is 'Route List Configuration'. There are several action buttons: Save, Delete, Copy, Reset, Apply Config, and Add New. The 'Status' section shows 'Status: Ready'. The 'Route List Information' section includes a checked box for 'Device is trusted', a text input for 'Name' containing 'RLAccesoPublicoGL', an empty text input for 'Description', a dropdown menu for 'Cisco Unified Communications Manager Group*' set to 'CMG_GLABPUBSUB', and a checked box for 'Enable this Route List (change effective on Save; no reset required)'. The 'Route List Member Information' section has a 'Selected Groups**' list containing 'Standard Local Route Group' and 'RG_B0_Central', with an 'Add Route Group' button and up/down arrows. Below it is an empty 'Removed Groups***' list. The 'Route List Details' section at the bottom shows a list of route groups: 'Standard Local Route Group' and 'RG_B0_Central'.

3.4.4.2.3 Route Patterns

Los route patterns son una cadena de dígitos que tienen una forma similar a 9.[2-9]XXXXXX, configuradas en el Call Manager para enrutar llamadas a entidades externas de la red. El route pattern puede apuntar directamente a un Gateway o bien a una lista de rutas, las cuales apunta a un grupo de rutas y finalmente éstas a un Gateway.

Para configurar un route pattern vamos a **Call Routing > Route/Hunt > Route Pattern > Add New**.

Una vez allí tendremos que configurar los siguientes parámetros:

- **Route Pattern:** escribiremos el patrón de llamada que estamos configurando.
- **Route Partition:** añadiremos uno de los route partition configurados anteriormente para poder restringir las llamadas que queramos o no restringir nada.
- **Description:** una descripción del route pattern para saber que hace rápidamente.
- **Gateway/Route List:** elegimos el Gateway por el que queramos que salga este tipo de llamadas.
- **Call Classification:** este parámetro lo pondremos siempre “Offnet” ya que la llamada esta enrutada fuera de nuestra red.

Por ejemplo para las llamadas nacionales el Route Pattern queda configurado:

The screenshot displays the 'Route Pattern Configuration' page in a web browser. The navigation menu at the top includes System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. Below the title bar, there are icons for Save, Delete, Copy, and Add New. The 'Status' section shows 'Status: Ready'. The 'Pattern Definition' section contains the following fields:

- Route Pattern*: 0.[8-9][^0]XXXXXXX
- Route Partition: Acceso Publico
- Description: Nacionales
- Numbering Plan: -- Not Selected --
- Route Filter: < None >
- MLPP Precedence*: Predeterminado
- Resource Priority Namespace Network Domain: < None >
- Gateway/Route List*: RLAccesoPublicoGL (Edit)
- Route Option: Route this pattern, Block this pattern Sin errores
- Call Classification*: OffNet
- Allow Device Override, Provide Outside Dial Tone, Allow Overlap Sending, Urgent Priority
- Require Forced Authorization Code
- Authorization Level*: 0
- Require Client Matter Code

The 'Calling Party Transformations' section includes:

- Use Calling Party's External Phone Number Mask
- Calling Party Transform Mask: [Empty field]
- Prefix Digits (Outgoing Calls): [Empty field]
- Calling Line ID Presentation*: Default
- Calling Name Presentation*: Default
- Calling Party Number Type*: Cisco CallManager
- Calling Party Numbering Plan*: Cisco CallManager

Y la lista de todos los Route Patterns es:

<input type="checkbox"/>	Pattern ^	Description	Partition	Route Filter	Associated Device
<input type="checkbox"/>	0.00!	Internacionales	Acceso Publico		RLAccesoPublicoGL
<input type="checkbox"/>	0.00!	Internacionales Restriccion	RestricInternacionales		RLAccesoPublicoGL
<input type="checkbox"/>	0.00!#	Internacionales	Acceso Publico		RLAccesoPublicoGL
<input type="checkbox"/>	0.00!#	Internacionales Restriccion	RestricInternacionales		RLAccesoPublicoGL
<input type="checkbox"/>	0.00350200XXXXX	LD Gibraltar	AllowGibraltar		RLAccesoPublicoGL
<input type="checkbox"/>	0.00350200XXXXX#	LD Gibraltar	AllowGibraltar		RLAccesoPublicoGL
<input type="checkbox"/>	0.090	Marcacion Datafonos	Acceso Publico		RLAccesoPublicoGL
<input type="checkbox"/>	0.0XX	Emergencias	Acceso Publico		RLAccesoPublicoGL
<input type="checkbox"/>	0.112	Emergencias	Acceso Publico		RLAccesoPublicoGL
<input type="checkbox"/>	0.118XX	Servicios Informacion Restric	RestricTarifEspecial		RLAccesoPublicoGL
<input type="checkbox"/>	0.118XX	Servicios Informacion	Acceso Publico		RLAccesoPublicoGL
<input type="checkbox"/>	0.1415	Datafonos con 0	Acceso Publico		RLAccesoPublicoGL
<input type="checkbox"/>	0.1XX	Servicios Especiales Restric	RestricNacionales		RLAccesoPublicoGL
<input type="checkbox"/>	0.1XX	Servicios Especiales	Acceso Publico		RLAccesoPublicoGL
<input type="checkbox"/>	0.[5-6]XXXXXXXXXX	Moviles Restriccion	RestricMoviles		RLAccesoPublicoGL
<input type="checkbox"/>	0.[5-6]XXXXXXXXXX	Moviles	VMMaskToMobile		RLMovilesGL
<input type="checkbox"/>	0.[5-6]XXXXXXXXXX	Moviles	Acceso Publico		RLMovilesGL
<input type="checkbox"/>	0.[8-9]0[0-2]XXXXXXXX	Nacionales Restriccion	RestricNacionales		RLAccesoPublicoGL
<input type="checkbox"/>	0.[8-9]0[0-2]XXXXXXXX	Nacionales	Acceso Publico		RLAccesoPublicoGL
<input type="checkbox"/>	0.[8-9]0[3-9]XXXXXXXX	Tarifacion Especial	Acceso Publico		RLAccesoPublicoGL
<input type="checkbox"/>	0.[8-9]0[3-9]XXXXXXXX	Tarifacion Especial Restric	RestricTarifEspecial		RLAccesoPublicoGL
<input type="checkbox"/>	0.[8-9][^0]XXXXXXXX	Nacionales	Acceso Publico		RLAccesoPublicoGL
<input type="checkbox"/>	0.[8-9][^0]XXXXXXXX	Nacionales Restriccion	RestricNacionales		RLAccesoPublicoGL
<input type="checkbox"/>	1100	Telefono RDSI Esplugues	InternasGLab		RL_GWB21
<input type="checkbox"/>	1415	Marcacion Datafonos	Acceso Publico		RLAccesoPublicoGL
<input type="checkbox"/>	4673	Telefono RDSI Alcobendas	InternasGLab		RL_GWM85
<input type="checkbox"/>	6XXXX	Moviles Internos	VMMaskToMobile		RLMovilesGL
<input type="checkbox"/>	6XXXX	Moviles Internos	InternasGLab		RLMovilesGL
<input type="checkbox"/>	7.160XXX	Marcacion a PATTON Lisboa	InternasGLab		10.35.1.208
<input type="checkbox"/>	80XX	Marcacion a Asterix	InternasGLab		Asterisk_trunk
<input type="checkbox"/>	87XX	Pruebas	InternasGLab		RL_GWB0
<input type="checkbox"/>	900876586	Marcacion Datafonos	Acceso Publico		RLAccesoPublicoGL
<input type="checkbox"/>	90102091[01]	Marcacion Datafonos	Acceso Publico		RLAccesoPublicoGL
<input type="checkbox"/>	901810252	Marcacion Datafonos	Acceso Publico		RLAccesoPublicoGL

Si nos fijamos en la tabla de Route Patterns hay uno especial que es 80XX, el cual tiene como Associated Device Asterisk_trunk. Esto es el SIP Trunk necesario para poder conectar el Cisco Call Manager con Asterisk y así poder realizar llamadas a extensiones entre ellos.

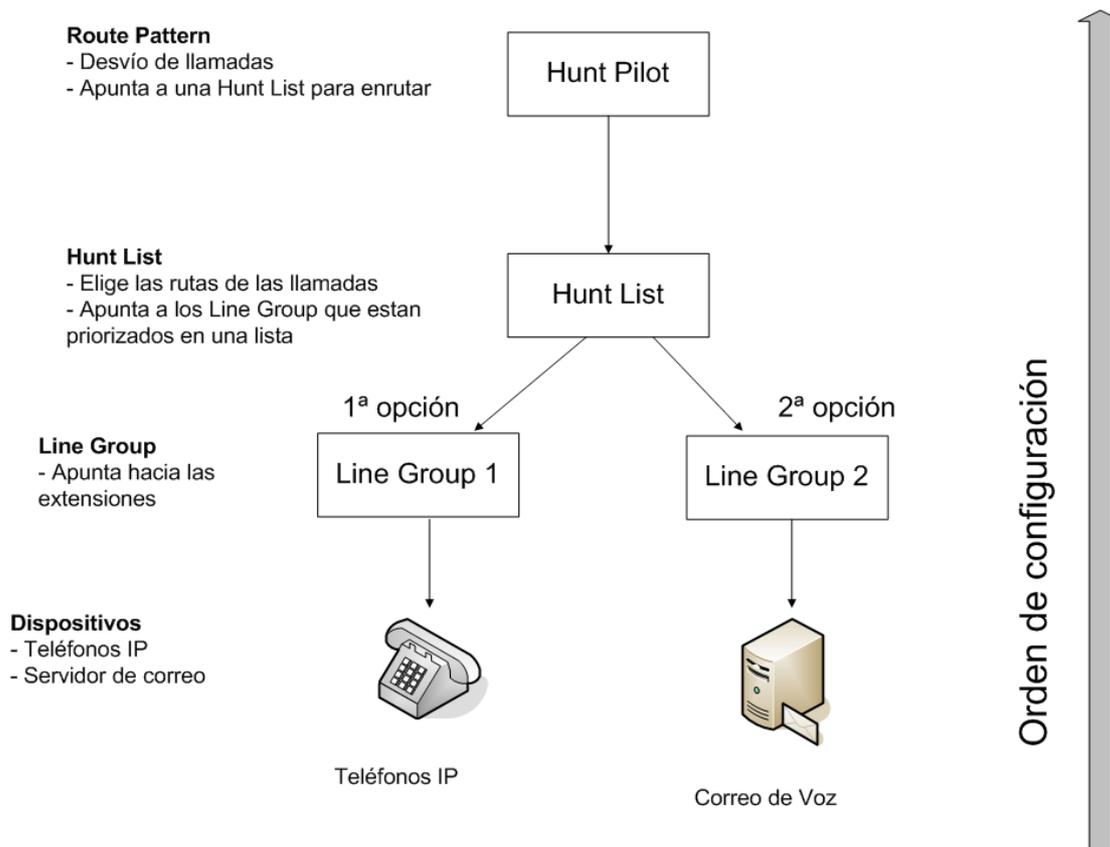
Este trunk se explicará más adelante como configurarlo.

3.4.4.3 Configuración de los Hunt List y Line Groups

Para distribuir las llamadas a través de un grupo de terminales utilizaremos una arquitectura de tres niveles, similar a la utilizada anteriormente para enrutar llamadas externas, la cual permite múltiples capas de enrutamiento de llamadas.

El Call Manager busca una coincidencia entre uno de los Hunt Pilots configurados y el número de la llamada entrante y utiliza esto para seleccionar la correspondiente Hunt List, la cual es una lista priorizada de rutas para realizar una llamada. Estas rutas se las conoce como Line Groups.

En la siguiente imagen podemos ver la arquitectura de tres niveles:



3.4.4.3.1 Line Group

Los miembros del Line Group son extensiones controladas por el Call Manager. Así cuando la llamada es distribuida a través del Line Group el Call Manager tiene el control de la llamada.

Se pueden aplicar múltiples opciones del Line Group cuando una llamada no se responde o cuando la extensión está ocupada o no registrada en el sistema.

Los Line Groups controlan el orden en que se distribuye la llamada, y tienen las siguientes características:

- Los Line Groups apuntan a extensiones específicas, las cuales son teléfono IP o puertos de correo de voz.
- Una extensión puede estar presente en múltiples Line Groups
- El Call Manager distribuye las llamadas acorde con el algoritmo de distribución asignado. El Call Manager soporta los siguientes algoritmos:

- Top-down
- Circular
- Mayor tiempo de inactividad
- Broadcast
- Si salta el evento de No-Contesta, Ocupado o No-Disponible, lo Line Groups redireccionan una llamada a una extensión basándose en las siguientes opciones:
 - Prueba siguiente miembro en la lista, y sino prueba el siguiente grupo de la lista de la Hunt List.
 - Prueba siguiente miembro en la lista, pero no saltes al siguiente grupo de la lista de la Hunt List.
 - Salta los siguientes miembros de la lista y vete directamente al siguiente grupo de la lista
 - Para todos los saltos.

Para configurar los Line Groups vamos a **Call Routing > Route/Hunt > Line Group > Add New**.

Una vez allí tenemos que configurar:

- **Line Group Name:** nombre que le daremos al Line Group
- **RNA Reversion Timeout:** es el tiempo, en segundos, que tiene que esperar el Call Manager para pasar la llamada a la siguiente extensión disponible de la lista o saltar al siguiente grupo según se haya configurado.
- **Distribution Algorithm:** elegimos el algoritmo de distribución que nos interese.
- **No Answer:** aquí configuramos el comportamiento que debe tener la llamada en caso de que la extensión a la que se llama no conteste.
- **Busy:** aquí configuramos el comportamiento que debe tener la llamada en caso de que la extensión a la que se llama este ocupada.
- **Not Available:** aquí configuramos el comportamiento que debe tener la llamada en caso de que la extensión a la que se llama no este disponible. Una extensión

no disponible es una extensión que por lo que sea no esta registrada en el Call Manager en eso momento.

En la siguiente imagen vemos la configuración de la Centralita de la sede central:

The screenshot shows the 'Line Group Configuration' page in Cisco Unified Communications Manager. The page is titled 'Line Group Configuration' and has a navigation bar at the top with menus for System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. Below the navigation bar, there are icons for Save, Delete, and Add New. The main configuration area is divided into three sections: 'Line Group Information', 'Hunt Options', and 'Line Group Member Information'.
Line Group Information: Line Group Name* is 'CentralitaB0', RNA Reversion Timeout* is '180', and Distribution Algorithm* is 'Broadcast'.
Hunt Options: No Answer*, Busy**, and Not Available** are all set to 'Try next member; then, try next group in Hunt List'.
Line Group Member Information: This section includes a 'Find Directory Numbers to Add to Line Group' area with a Partition dropdown set to '< None >', a Directory Number Contains field, and a Find button. Below this is a list of Available DN/Route Partitions: 1000/InternasGLab, 1001/InternasGLab, 1002/InternasGLab, 1101/InternasGLab, and 1102/InternasGLab. An 'Add to Line Group' button is present. The 'Current Line Group Members' section has a 'Reverse Order of Selected DN/Route Partitions' button. The Selected DN/Route Partition list contains 4000/InternasGLab, 4001/InternasGLab, and 4002/InternasGLab. The Removed DN/Route Partition list is empty.

Vemos que se a configurado que si la extensión a la que se llama es la 4000 no contesta, esta ocupada o no esta disponible al cabo de 180 segundos salta automáticamente a la extensión 4001 y sino a la 4002.

Este proceso lo haremos para todas las extensiones o grupo de extensiones de departamentos que queramos hacer un grupo de salto.

3.4.4.3.2 Hunt List

Una Hunt List es una lista priorizada de rutas (Line Groups) para poder realizar una llamada.

Las Hunt Lists tienen las siguientes características:

- Múltiples Hunt Pilots pueden apuntar a una misma Hunt List.
- Una Hunt List es una lista priorizada de Line Groups que funcionan como alternativa a otro grupo configurado en la Hunt List. Por ejemplo, se puede configurar un grupo para poder coger una llamada. Si la llamada no se coge entonces en la Hunt Lists puede haber configurado otro Line Group y la llamada pasaría a éste segundo grupo de extensiones.
- Múltiples Hunt Lists pueden contener el mismo Hunt Lists.

Para configurar los Line Groups vamos a **Call Routing > Route/Hunt > Hunt List > Add New**.

Una vez allí tenemos que configurar:

- **Name:** nombre que le daremos a la Hunt List.
- **Description:** descripción de la Hunt List
- **Selected Groups:** Añadimos los Line Groups que queramos utilizar y en el orden que queramos que salten de un grupo al otro al elegir la Hunt List.

En la siguiente figura vemos la configuración de Hunt List del grupo de Dirección:

The screenshot displays the 'Hunt List Configuration' page. At the top, there is a navigation menu with options like System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. Below the navigation is a toolbar with icons for Save, Delete, Copy, Reset, Apply Config, and Add New. The main content area is divided into several sections:

- Status:** Shows 'Status: Ready' with an information icon.
- Hunt List Information:** Contains fields for Name (HL Direccion B21-B0), Description (Llamadas al DDI 6062 en Espligues), and Cisco Unified Communications Manager Group (CMG_GLABSUBPUB). There are also checkboxes for 'Device is trusted', 'Enable this Hunt List (change effective on Save; no reset required)', and 'For Voice Mail Usage'.
- Hunt List Member Information:** Features an 'Add Line Group' button and two list boxes. The 'Selected Groups**' list contains 'Direccion_B21_B0' and 'CentralitaB0'. The 'Removed Groups***' list is empty.
- Hunt List Details:** Shows a list of groups: 'Direccion_B21_B0' and 'CentralitaB0'.

At the bottom of the page, there is another set of buttons: Save, Delete, Copy, Reset, Apply Config, and Add New.

Vemos que tiene configurado que cuando entre una llamada a ese Hunt List primero intentara pasarla a la Line Group de Dirección y si nadie la coge o están ocupados pasa la llamada al grupo de Centralita de la sede central.

Como hemos visto en la sección anterior las Line Group están configuradas con una lista de extensiones con prioridad.

3.4.4.3.3 Hunt Pilot

Hunt Pilots son cadenas de dígitos y caracteres especiales parecidos a los Route Pattern (9.[2-9]XXXXXX), los cuales se utilizan para enrutar llamadas hacia los Hunt List.

Lo que conseguimos con los Hunt Pilots es poder llamar a una extensión que no tiene porque tener asociado un teléfono físico, pero sí que al llamar a ese número nos pase directamente a un grupo de teléfonos de un departamento como puede ser que por ejemplo llames a la extensión 2299, configurada en el Hunt Pilot y que dicha extensión apunte a la Hunt List de Atención al Usuario. Esta Hunt List de atención al usuario tiene

configurada un Line Group con una lista priorizada de las extensiones del departamento de atención al usuario.

Vamos a ver las configuraciones. La primera imagen nos enseña la configuración del Hunt Pilot de la extensión 2299:

The screenshot displays the 'Hunt Pilot Configuration' page. At the top, there is a navigation menu with items: System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. Below the menu is a dark header with the title 'Hunt Pilot Configuration'. Underneath the header is a toolbar with icons for Save, Delete, Copy, and Add New. The main content area is divided into three sections:

- Status:** Shows an information icon and the text 'Status: Ready'.
- Pattern Definition:** Contains several fields:
 - Hunt Pilot*: 2299
 - Route Partition: InternasGLab
 - Description: HP Atencion Usuario Barcelona Int
 - Numbering Plan: < None >
 - Route Filter: < None >
 - MLPP Precedence*: Predeterminado
 - Hunt List*: HL Atencion-Usuario Int B0 (with an Edit link)
 - Route Option: Radio buttons for 'Route this pattern' (selected) and 'Block this pattern' (with a dropdown menu showing 'Sin errores').
 - Checkboxes for 'Provide Outside Dial Tone' and 'Urgent Priority'.
- Hunt Forward Settings:** Contains a table with columns 'Use Personal Preferences' and 'Destination'.

	Use Personal Preferences	Destination
Forward Hunt No Answer	<input type="checkbox"/> or	<input type="text"/>
Forward Hunt Busy	<input type="checkbox"/> or	<input type="text"/>
Call Pickup Group	Informatica_1 in InternasGLab	
Maximum Hunt Timer	<input type="text"/>	

Vemos que hay que configurar los dígitos que nos interesen para hacer el Hunt Pilot, la Route partition, una descripción de lo que hace y la parte importante la Hunt List que asociamos al Hunt Pilot que estamos configurando.

En la siguiente imagen vemos la configuración del Hunt List HL Atencion-Usuario Int B0.

The screenshot shows the configuration page for a Hunt List. It is divided into three main sections:

- Status:** Shows an information icon and the text "Status: Ready".
- Hunt List Information:** Contains several fields and checkboxes:
 - Device is trusted
 - Name*: HL Atencion-Usuario Int B0
 - Description: HL Atencion Usuario B0
 - Cisco Unified Communications Manager Group*: CMG_GLABPUBSUB (dropdown menu)
 - Enable this Hunt List (change effective on Save; no reset required)
 - For Voice Mail Usage
- Hunt List Member Information:** Contains a button "Add Line Group" and two list boxes:
 - Selected Groups**: A list box containing "Atencion-Usuario_B0".
 - Removed Groups***: An empty list box.

Vemos que tan solo tiene configurado el Line Group Atencion-Usuario_B0, si vamos a dicho Line Group vemos que se tiene configuradas las extensiones de la 2200 a la 2214 que son las extensiones de atención al usuario e informatica.

The screenshot shows the configuration page for a Line Group. It is divided into three main sections:

- Line Group Information:** Contains fields for:
 - Line Group Name*: Atencion-Usuario_B0
 - RNA Reversion Timeout*: 15
 - Distribution Algorithm*: Circular (dropdown menu)
- Hunt Options:** Contains three dropdown menus:
 - No Answer*: Try next member; then, try next group in Hunt List
 - Busy**: Try next member; then, try next group in Hunt List
 - Not Available**: Try next member; then, try next group in Hunt List
- Line Group Member Information:** Contains a section for finding directory numbers:
 - Find Directory Numbers to Add to Line Group:
 - Partition: < None >
 - Directory Number Contains: (empty field)
 - Find: (button)
 - Available DN/Route Partition: List of 1000/InternasGLab, 1001/InternasGLab, 1002/InternasGLab, 1101/InternasGLab, 1102/InternasGLab.
 - Add to Line Group: (button)
 - Current Line Group Members:
 - Reverse Order of Selected DN/Route Partitions: (button)
 - Selected DN/Route Partition: List of 2200/InternasGLab, 2201/InternasGLab, 2202/InternasGLab, 2203/InternasGLab, 2204/InternasGLab.

Por lo tanto, si un usuario llama a la extensión 2299 querrá decir que quiere hablar con alguien de atención al usuario y el primer teléfono que sonará si no esta ocupado es el 2200, si éste esta ocupado, nadie lo coge o esta desconectado, se llamará al 2201 y así consecutivamente hasta el 2214.

Al tener un algoritmo de distribución circular si al llegar al 2214 tampoco se ha conseguido realizar la llamada se volverá a intentar conectar al 2200 otra vez.

3.4.5 Trunk entre Cisco Call Manager y Asterisk

Para poder conectar las dos centralitas telefónicas necesitamos hacer un trunk SIP entre ellas dos.

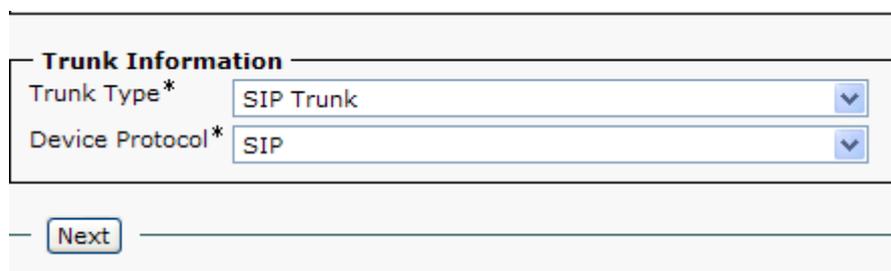
Tenemos que configurar un trunk de Cisco a Asterisk y otro entre Asterisk y Cisco. En esta sección explicaremos el trunk entre Cisco y Asterisk.

Primero explicaremos como funciona la telefonía entre las dos centralitas. Siempre que haya llamadas entre extensiones configuradas en las mismas centralitas las llamadas las controlará dicha centralita. Si hay una llamada entre una extensión configurada en Asterisk y una extensión configurada en Cisco y al revés la llamada se realizará a través del trunk.

Por último, si hay una llamada entre la centralita Asterisk y un número externo los permisos y la conexión de esa llamada los lleva el Cisco Call Manager.

Para configurar el trunk vamos a **Device > Trunk > Add New**.

En la primera pantalla nos pregunta que tipo de trunk queremos configurar, elegimos SIP Trunk:



The image shows a configuration window titled "Trunk Information". It contains two dropdown menus: "Trunk Type*" is set to "SIP Trunk" and "Device Protocol*" is set to "SIP". Below the dropdowns is a "Next" button.

Una vez dentro tenemos que configurar:

- **Device Name:** nombre que le queremos dar al trunk.

- **Description:** descripción del trunk por si tenemos varios para identificar que hace rápidamente.
- **Device Pool:** la dejaremos en Default.
- **Call Classification:** aquí elegiremos el parámetro OnNet ya que estamos realizando la llamada a través del trunk por la red interna.
- Clickamos para que este activa la casilla **Media Termination Point Required**.
- **Inbound Calls > Calling Search Space:** elegimos del desplegable CSSTotal ya que no queremos restricciones par alas extensions de Asterisk.
- **SIP Information > Destination Address:** aquí tenemos que poner la dirección IP del servidor Asterisk, en nuestro caso es 10.1.21.20.
- **SIP Information > MTP Preferred Originating Codec:** elegiremos el codec 711ulaw.
- **SIP Information > SIP Trunk Security Profile:** elegimos la Non Secure SIP Trunk Profile ya que no queremos ningun tipo de autenticación.
- **SIP Information > SIP Profile:** elegimos la Standard SIP Profile.

Por lo tanto la configuración del SIP Trunk queda:

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Trunk Configuration

Save Delete Reset Apply Config Add New

Device Information

Product: SIP Trunk
 Device Protocol: SIP
 Device Name*: Asterisk_trunk
 Description: Trunk Cisco a Asterisk
 Device Pool*: Default
 Common Device Configuration: < None >
 Call Classification*: OnNet
 Media Resource Group List: < None >
 Location*: Hub_None
 AAR Group: < None >
 Packet Capture Mode*: None
 Packet Capture Duration: 0

Media Termination Point Required
 Retry Video Call as Audio
 Transmit UTF-8 for Calling Party Name
 Unattended Port
 SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose ke
 Use Trusted Relay Point* Predeterminado

Incoming Calling Party Settings

If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.

Number Type	Prefix	Strip Digits	Use Device Pool CSS
Unknown Number	Default	0	<input checked="" type="checkbox"/>

Multilevel Precedence and Preemption (MLPP) Information

MLPP Domain: < None >

Call Routing Information

Remote-Party-Id
 Asserted-Identity
 Asserted-Type*: Predeterminado
 SIP Privacy*: Predeterminado

Inbound Calls

Significant Digits*: All
 Connected Line ID Presentation*: Default
 Connected Name Presentation*: Default
 Calling Search Space: CSSTotal
 AAR Calling Search Space: < None >
 Prefix DN:
 Redirecting Diversion Header Delivery - Inbound

Outbound Calls

Called Party Transformation CSS: < None >
 Use Device Pool Called Party Transformation CSS
 Calling Party Transformation CSS: < None >
 Use Device Pool Calling Party Transformation CSS
 Calling Party Selection*: Originator
 Calling Line ID Presentation*: Default
 Calling Name Presentation*: Default
 Caller ID DN:
 Caller Name:
 Redirecting Diversion Header Delivery - Outbound

SIP Information	
Destination Address	<input type="text" value="10.1.21.20"/>
Destination Address IPv6	<input type="text"/>
<input type="checkbox"/> Destination Address is an SRV	
Destination Port*	<input type="text" value="5060"/>
MTP Preferred Originating Codec*	<input type="text" value="711ulaw"/>
Presence Group*	<input type="text" value="Standard Presence group"/>
SIP Trunk Security Profile*	<input type="text" value="Non Secure SIP Trunk Profile"/>
Rerouting Calling Search Space	<input type="text" value="< None >"/>
Out-Of-Dialog Refer Calling Search Space	<input type="text" value="< None >"/>
SUBSCRIBE Calling Search Space	<input type="text" value="< None >"/>
SIP Profile*	<input type="text" value="Standard SIP Profile"/>
DTMF Signaling Method*	<input type="text" value="Sin preferencias"/>

Geolocation Configuration	
Geolocation	<input type="text" value="< None >"/>
Geolocation Filter	<input type="text" value="< None >"/>
<input type="checkbox"/> Send Geolocation Information	

4 TELEFONÍA ASTERISK

4.1 Introducción

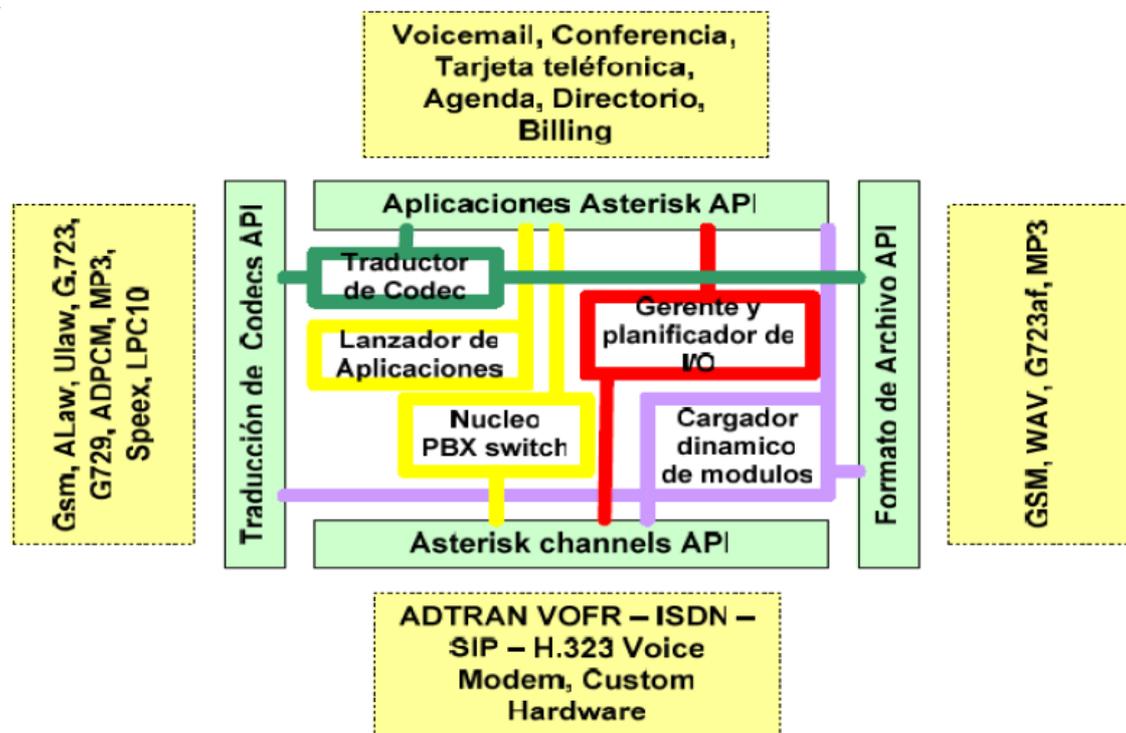
4.1.1 ¿Qué es Asterisk?

Asterisk es una aplicación para controlar y gestionar comunicaciones de cualquier tipo, ya sean analógicas, digitales o VoIP mediante todos los protocolos VoIP que implementa.

Asterisk es un software que usa licencia de software libre (GPL). Digium es la empresa que lo promueve e invierte tanto en el desarrollo del software como de hardware de bajo coste que funciona con Asterisk.

Asterisk permite la conectividad en tiempo real entre las redes PSTN y redes VoIP.

4.1.2 Arquitectura de Asterisk



Arquitectura de Asterisk – Fuente: <http://www.redesymas.org/2011/07/caracteristicas-de-asterisk-linux.html>

La arquitectura de Asterisk está formada por cuatro APIs. Un API es el conjunto de funciones y procedimientos que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción.

Descripción de las APIs:

- **API de Canales**

Un canal es el equivalente a una línea telefónica en la forma de un circuito de voz digital. Es decir, Maneja el tipo de conexión por el cual el cliente está llegando sea una conexión SIP, H323, RDSI, etc.

- **API de traducción de Codecs**

Carga módulos, codecs, para apoyar varios tipos de audio, codificando y decodificando formatos tales como G711, G729, GSM23, etc.

- **API formato de archivo**

Maneja la lectura y escritura de varios formatos de archivos para el almacenaje de datos en el sistema de archivos.

- **API Aplicaciones**

Permite a varios módulos de tareas cumplir varias funciones, multiconferencias, lista de directorios, buzones de voz, aplicaciones personalizadas, etc.

4.1.3 Integración de Asterisk con Cisco

Para poder realizar llamadas a cualquier extensión de la compañía tenemos que integrar la centralita Asterisk en la estructura de red ya configurada para la centralita Cisco.

Cuando haya un centro con teléfonos IP que no sean Cisco, estos teléfonos tienen que poder llegar a Asterisk para configurarlos y que la centralita lleve toda la señalización de la llamada.

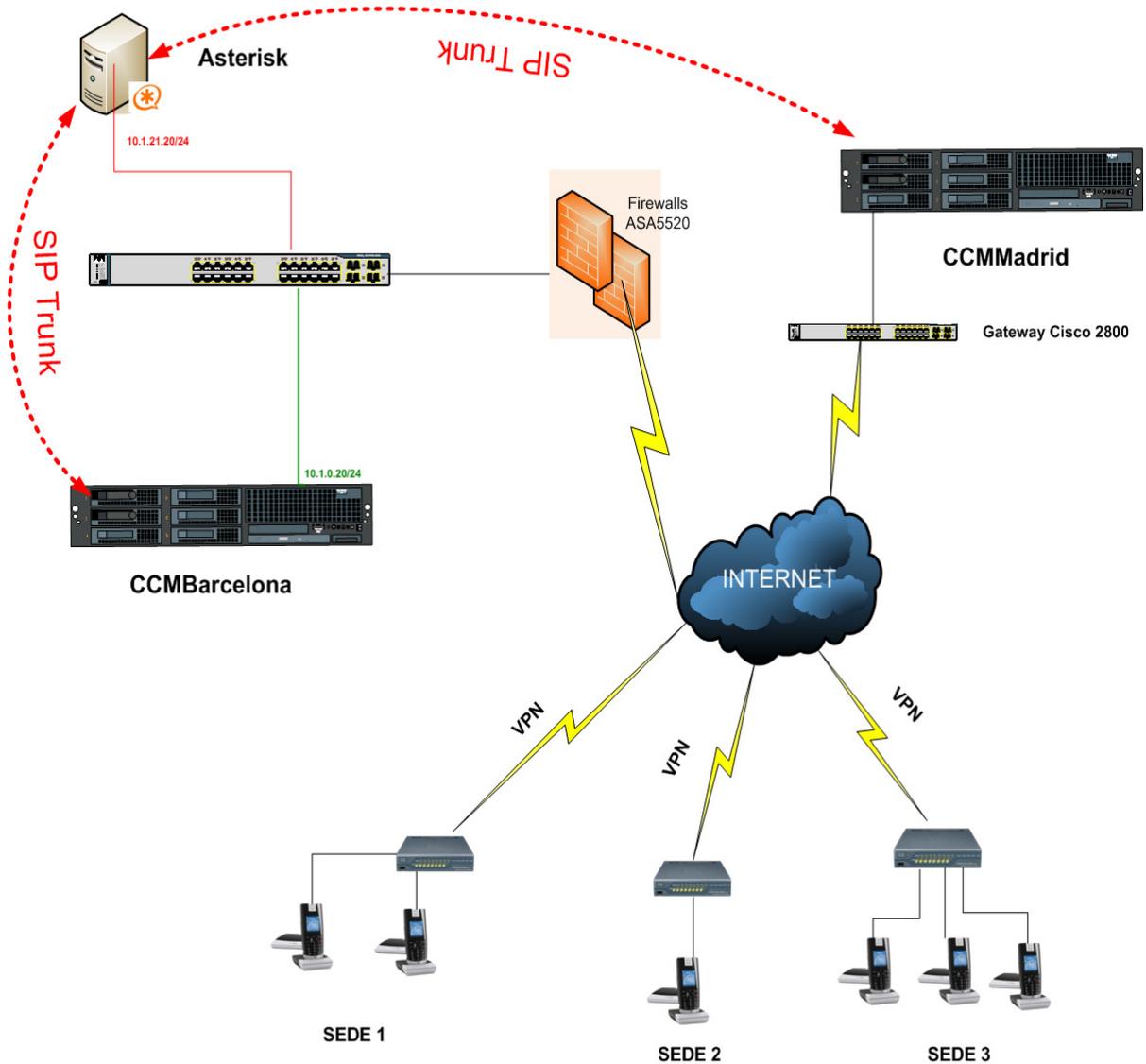
Una vez configurado el teléfono y tenga conexión con Asterisk, entre Asterisk y Cisco habrá una conexión SIP Trunk entre ellos así de esta forma se podrán realizar llamadas entre extensiones de uno y otro sin problemas.

Hay dos Cisco Call Manager, uno se encuentra en Barcelona y el otro en Madrid. Ambos están conectados en cluster. Para asegurar la conectividad con Asterisk

deberemos crear dos trunk uno entre Barcelona y el Asterisk, y otro entre Madrid y Asterisk.

Los teléfonos conectados a Asterisk se conectarán a un cisco ASA en el mismo centro y de allí mediante VPN llegarán a los ASAs de la sede central. Éstos ASAs enrutarán el tráfico hasta Asterisk y ya estarán conectados.

En la siguiente figura podemos ver una imagen de ésta estructura simplificada.



4.1.4 Administración de Asterisk

La administración de Asterisk puede realizarse a través de web o a través de línea de comandos CLI¹⁷.

Asterisk CLI es la consola desde la que podemos controlar y monitorizar gran parte de la situación de la centralita. Para entrar tenemos que escribir por línea de comandos **asterisk -r**

Como comandos principales tenemos:

- Versión instalada: **core show version**
- Tiempo de ejecución después del último reinicio: **core show uptime**
- Detener Asterisk al momento: **core stop now**
- Detener Asterisk cuando no haya carga: **core stop when convenient**
- Detener Asterisk cuando no haya carga y dejar de aceptar peticiones de llamadas a partir de ese momento: **core stop gracefully**
- Nivel de “Verbose”: Este valor indica la cantidad de mensajes que se recibirán sobre los eventos generales del sistema. Cuanto más alto, más información sobre lo que sucede en la centralita se recibirá.

Este nivel, se puede establecer de varias formas:

- Al arrancar el daemon: **sudo asterisk vvvvvv**
- Al conectarse al daemon: **sudo asterisk rvvvvvvvv**
- Desde el CLI: **Set Verbose 30**

4.1.5 Ficheros de configuración Asterisk

Asterisk se configura desde múltiples ficheros de configuración, los más importantes son:

- Fichero de configuración principal: **asterisk.conf**

¹⁷ Command Line Interface

- Fichero de configuración de módulos: **modules.conf**
- Canales:
 - **iax.conf**: Canales Inter Asterisk eXchange
 - **sip.conf**: Canales SIP
 - **zapata.conf**: Telefonía analógica y digital
 - **h323.conf**: Canales H.323
- Dialplan:
 - **extensions.conf**: El propio Dialplan, donde están configuradas todos los tipos de extensiones.
- Configuración de aplicaciones del Dialplan:
 - **meetme.conf**: Para sala de conferencias.
 - **musiconhold.conf**: Configuración de la música en espera.
 - **queues.conf**: Configuración de colas de llamadas.
 - **voicemail.conf**: Configuración de los buzones de voz.

4.1.5.1 El archivo sip.conf

Como todas las extensiones que definiremos en el proyecto serán SIP, vamos a profundizar en el archivo sip.conf.

En este fichero se definen:

- Variables generales de SIP
- Clientes SIP
- Servidores SIP

En primer lugar existe la sección [general], donde se definen variables globales y aspectos por defecto para todos los canales SIP. La sintaxis es la siguiente:

[general]

variable1=valor1

variable2=valor2

Las variables globales más utilizadas son:

- **allow/disallow**: indican los codecs permitidos/no permitidos.
- **dtmfmode**: permite especificar el método por el cual se enviarán los tonos (dígitos pulsados durante la conversación).
- **nat**: informa a Asterisk del tipo de NAT en el que se encuentra.
- **externip**: Dirección pública del NAT.
- **context**: Contexto por defecto donde entrarán las llamadas entrantes.
- **port**: Puerto por el que escuchar. Por defecto esta configurado el puerto 5060.

4.1.5.1.1 Clientes y servidores en sip.conf

En sip.conf se definen tanto los clientes que se conectarán a Asterisk, como los proveedores que se utilizaran para encaminar llamadas. Conceptualmente, se distingue:

- **user**: Envía llamadas a Asterisk
- **peer**: Recibe llamadas de Asterisk (proveedor).
- **friend**: Recibe y Envía llamadas (usuario).

La syntaxis para definir un friend o un peer es:

[nombre]

type = friend / peer

variable = valor

variable2 = valor

....

Las variables más importantes que deben ser configuradas inicialmente son:

- **type: peer / friend**. El parámetro friend se utiliza cuando la extensión es un teléfono y peer es para cuando el dispositivo SIP puede llevar llamadas, como un Trunk.
- **context**: Contexto donde entraran las llamadas generadas.
- **nat**: Indica si el usuario o peer se encuentran tras un nat.

- **host**: IP dinámica o estática para la extensión. Si ponemos el puerto en dinámico permitiremos que cualquier dispositivo pueda pasar la autenticación SIP para poder realizar y recibir llamadas, por lo que configuraremos siempre los teléfonos en dinámico.
- **username**: nombre de usuario.
- **secret**: contraseña de acceso.
- **allow y disallow**: Configuraciones de codecs específicas para cada friend/peer.
- **qualify**: Evalúa el estado del extremo SIP para conocer su accesibilidad y latencia.

En nuestro servidor el archivo de configuraciones de extensiones y trunks se encuentra en `/etc/asterisk/sip_additional.conf`.

Como ejemplo la extensión 8001 queda:

[8001]	//Nombre de la extensión
secret=8001	// Password para conectar el teléfono
dtmfmode=rfc2833	//Protocolo de señalización de la extensión por defecto es rfc2833
canreinvite=no	//Con esta opción indicamos a Asterisk que no envíe paquetes “reinvite” a no ser que sea necesario
context=from-internal	//Es el contexto al que puede llamar la extensión, todas las extensiones por defecto están en el contexto from-internal
host=dynamic	//Como queremos que el teléfono se registre solo, ponemos IP dinámica
trustpid=yes	// Decimos que el teléfono es de confianza
sendrpid=no	//Poniendo el parámetro a “no”, no dejamos que se mande la cabecera SIP
type=friend	//Todos los teléfonos tienen que estar configurados como friend
nat=no	//No hay nat en la conexión de la extensión con Asterisk
port=5060	//Puerto de comunicación con el servidor
qualify=yes	// Tiempo de latencia no superior a 2000ms
qualifyfreq=60	//Chequea cada 60 segundos si se puede alcanzar la extensión
transport=udp	//Protocolo utilizado para la comunicación
encryption=no	//Llamada sin encriptación
callgroup=	//La extensión no está configurada en ningún grupo de salto
pickupgroup=	//La extensión no está configurada en ningún grupo de cogida
dial=SIP/8001	//Indica que para llamar hay que marcar la extensión 8001

mailbox=8001@device	//Configuracio de la bandeja de mail de ese dispositivo
permit=0.0.0.0/0.0.0.0	//Permitimos que se pueda llamar a dicha extensión desde cualquier red
callerid=device <8001>	//Nombre de usuario y extension
faxdetect=no	//Indicamos que no es una extensión para fax

Cada extension se define con el número de extensión entre claudators.

Como las extensiones no necesitan ningún nat para llegar a Asterisk ponemos el parámetros “nat=no”.

Se puede monitorizar la latencia entre Asterisk y el teléfono/punto en cuestión mediante el parámetro “qualify=YES” para determinar si el dispositivo esta disponible, para este caso, Asterisk determina que para que un dispositivo sea operativo tiene que tener una latencia inferior a 2000ms.

El campo “host=dynamic” significa que el teléfono puede conectarse desde cualquier IP, esto se puede limitar mediante una IP fija o un nombre de dominio.

El parámetro “careinvite” se refiere a que cuando dos usuarios han establecido conexión entre ellos, los paquetes RTP de audio se envían directamente entre ellos sin pasar por el servidor Asterisk.

El parámetro de “context=from-internal” marca donde entrara la llamada que provenga de este elemento sip.

Con el parámetro “permit=0.0.0.0/0.0.0.0” dejamos que se pueda conectar la extensión desde cualquier red. Podemos limitar el acceso poniendo una dirección ip y una mascara.

Y la configuración del trunk entre Asterisk y el Call Manager:

[CallManagerBcn]	
disallow=all	//Deshabilitamos todos los codecs para poder despues habilitar solo uno
type=peer	//Como es un trunk se tiene que definir el tipo de conexión como peer
qualify=yes	//Este qualify es igual que antes con las extensiones, configuramos la latencia a 2000ms
nat=no	//No hay nat en la conexión de trunk con Cisco
insecure=port,invite	//Ignora la autenticación del puerto y no pide autenticación de paquetes INVITE
host=10.1.0.20	//Dirección IP del host con el que conecta el trunk
dtmf=rfc2833	//Protocolo de señalización de la extensión por defecto es rfc2833

context=from-internal	//Es el contexto al que puede llamar la extensión, todas las extensiones por defecto están en el contexto from-internal
canreinvite=no	//Con esta opción indicamos a Asterisk que no envíe paquetes “reinvite” a no ser que sea necesario
allow=ulaw	//Con esta opción activamos el codec ulaw . Este codec es el G.711, el cual utiliza 64kbps para cada lado de la llamada

Primero deshabilitamos todos los códecs, ya que para activar un códec primero hay que desactivar todos. Después activamos el códec “ulaw” que es el que Cisco admite y así poder tener una buena comunicación.

Para poder tener comunicación con Cisco también hay que crear una comunicación sin autenticación por eso se configura “insecure=port,invite”.

4.1.5.2 El Dialplan

Una vez configurados los usuarios y los proveedores externos tenemos que configurar qué sucederá cuando uno de estos usuarios marque alguna extensión. Esto lo configuraremos en el fichero **extensions.conf**.

Este fichero de configuración es el más importante de Asterisk, en él reflejaremos el plan de numeración de la centralita telefónica para cada contexto y usuario.

Como todos los archivos de configuración de Asterisk, extensions se divide en contextos que se marcan con su nombre entre corchetes y finalizarán cuando empiece otro contexto. Como en todos, cada uno de ellos tendrá su configuración independiente.

Hay dos contextos especiales reservados por el sistema que siempre, se utilicen o no, tienen que estar establecidos. Estos son el [general] y el [globals]. En el primero se configuran las opciones que tendrán todos los contextos y en [globals] tendremos todas las opciones que podrán ser utilizadas en el resto de contextos.

La sintaxis dentro del fichero **extensions.conf** sería:

exten => nombre,prioridad,aplicación(parámetros)
exten hace referencia a una extensión
prioridad al orden en que se ejecutan los comandos
aplicación es la acción que se quiere realizar

La prioridad comienza con 1 y se ejecuta en orden numérico. Cada prioridad ejecuta una aplicación. Asterisk introduce el uso de la prioridad n (next). Cada vez que encuentra una prioridad n, toma el número de prioridad anterior y le suma 1. Simplifica el proceso de la escritura cuando hay que añadir muchas extensiones.

Las aplicaciones más importantes son:

- **Authenticate (password | opciones):** Pide al usuario que introduzca una contraseña (siendo password la contraseña esperada). La opción más importante puede ser “j” que indica a Asterisk que debe saltar a la prioridad n + 101 si la autenticación falla.
- **Wait (n):** Espera n segundos, ignorando los dígitos marcados durante la llamada.
- **WaitExten (n):** Espera n segundos, pero gestionando los dígitos marcados.
- **WaitMusicOnHold(n):** Reproduce música en espera durante n segundos.
- **Answer():** Acepta la llamada entrante por el canal.
- **Busy():** Envía la señal de ocupado al origen.
- **Hangup():** Cuelga la llamada.
- **Ringin():** Envía la señal de tono de llamada.
- **DigitTimeout (segundos):** Establece el tiempo de espera máximo cuando el origen de la llamada marca una extensión (para detectar el fin de cadena).
- **Goto (contexto, extension, prioridad):** Salta al contexto, extensión y prioridad del argumento.
- **GotoIf (condicion ? prioridad1 : prioridad2):** Salta a la prioridad1 si la condición se cumple o salta a la prioridad2 si la condición no se cumple.

En el caso de llamadas internas o funcionamiento simple, las extensiones son conocidas. ¿Pero que pasa cuando un usuario llama a un número que no conoce el sistema? La solución es utilizar patrones en las extensiones.

Para indicar patrones, se utiliza el carácter: “_”

Se pueden utilizar:

- X: Indica un dígito del 0 al 9

- Z: Indica un dígito del 1 al 9
- N: Indica un dígito del 2 al 9
- [129] Indica el 1, 2 o 9
- . Indica uno o más caracteres

Ejemplos:

Fijos Nacionales: **exten=> _9XXXXXXXXX**

Internacionales: **exten=> _00.**

La configuración del Dialplan lo podemos encontrar en **/etc/asterisk/extensions_additional.conf**.

Como hay demasiadas configuraciones dentro del extensions veremos un pequeño ejemplo del formato interno del archivo extensions_additional.conf.

En el siguiente ejemplo vemos la configuración que se aplica cuando se marca la extensión 8001.

```
exten => 8001,1,Set(RingGroupMethod=none)
exten => 8001,n,Macro(record-enable,8001,IN)
exten => 8001,n,Macro(dial-one,,${DIAL_OPTIONS},8001)
exten => 8001,n,Hangup
```

Vemos que la primera prioridad es ir al RingGroupMethod, es decir va a buscar si esta extensión esta en un grupo de salto. Pero podemos ver que la variable esta a none, por lo que por aquí no entra.

La siguiente prioridad es ejecutar la Macro(record-enable), la cual si hemos dado la opción de grabar la llamada, ésta se grabará.

En la siguiente prioridad se mete en la Macro de dial-one, en la cual se llama al número marcado, ejecuta las opciones que la extensión tiene configuradas y enrutará las llamadas por donde tienen que pasar.

Si después de hacer esto no se logra realizar la llamada, esta se cuelga (Hangup).

4.1.5.3 Las colas

Las colas de llamadas se encuentran en el archivo `queues_additional.conf`.

Para abrir el archivo donde se encuentran esta en `/etc/asterisk/queues_additional.conf`.

En el siguiente cuadro vemos un ejemplo de una cola configurada.

```
[8010]
announce-frequency=0 //Poniendo a cero esta opción, no se anuncia el
                        tiempo estimado de espera a la persona que esta
                        esperando en la cola
announce-holdtime=no //No se anuncia el tiempo de espera en la cola
announce-position=no //No se anuncia a la persona que llama, la
                        posición que tiene en la cola
eventmemberstatus=no
eventwhencalled=no
joinempty=yes //La persona que llama puede entrar en una cola
               que no tiene miembros
leavewhenempty=no
maxlen=0
memberdelay=0
penaltymemberslimit=0
periodic-announce-frequency=15 //Es la frecuencia en segundos con la que se
                                anuncia el mensaje de espera que configuramos
                                para la cola
queue-callswaiting=silence/1
queue-thereare=silence/1
queue-youarenext=silence/1
reporholdtime=no
retry=5
ringinuse=yes
servicelevel=60
strategy=ringall //Es la estrategia que utilizamos cuando alguien
                  llama a la cola. En este caso hemos puesto que
```

suenen todas las extensiones que estan configuradas en la cola.

timeout=15

//Tiempo en segundos que queremos que suene una llamada antes de que se considere fallida

timeoutpriority=app

timeoutrestart=no

weight=0

wrapuptime=0

context=ivr-2

periodic-announce=custom/Espera //Es la locución que hemos elegido que se repita mientras la persona que llama espera.

member=Local/8000@from-queue/n,0,Centralita,hint:8000@ext-local //Aquí estan las extensiones configuradas en esta cola. En este caso solo hay una la 8000

4.2 Preparación del sistema

4.2.1 Hardware utilizado

En la documentación sobre Asterisk hemos visto una serie de requisitos mínimos para que Asterisk funcione, estos son un procesador de 500MHz PentiumIII, con 128MB de RAM y 2Gb de disco duro.

Cabe decir que cuanto mejor y más rápido sea el sistema utilizado para albergar Asterisk, mayor cantidad de llamadas simultáneas podrán ser albergadas.

Como hardware para albergar la instalación, por lo tanto, hemos elegido un servidor HP ProLiant DL140 G3, el cual tiene como características principales:

- Procesador: Procesador Intel Xeon 5310 Dual Core a 1.60 GHz.
- 2 Gb de memoria RAM
- Unidad de disco SATA de 80gb a 7.200 r.p.m.
- Puertos:
 - 2 x Red RJ-45 (Ethernet). Puertos para tarjetas de interfaz de red 10/100/1000
 - 1 x Serie.
 - 1 x Dispositivo de puntero (ratón).
 - 1 x Gráficos.
 - 1 x Teclado.
 - 4 x USB (2 frontales, 2 posteriores)

4.2.2 Elección del software

La elección del sistema operativo debe tener en cuenta las necesidades y los requisitos del sistema y de sus funcionalidades.

Debido a que Asterisk tiene que correr en un servidor con sistema operativo Linux deberemos elegir una distribución de este sistema. A continuación detallamos algunas de ellas:

- **Debian** es una comunidad conformada por desarrolladores y usuarios, que mantiene un sistema operativo GNU basado en software libre. El sistema se encuentra precompilado, empaquetado y en un formato .deb para múltiples arquitecturas de computador y para varios núcleos.

Nació como una apuesta por separar en sus versiones el software libre del software no libre. El modelo de desarrollo del proyecto es ajeno a motivos empresariales o comerciales, siendo llevado adelante por los propios usuarios, aunque cuenta con el apoyo de varias empresas en forma de infraestructuras. Debian no vende directamente su software, lo pone a disposición de cualquiera en Internet.



- **SUSE Linux** es una de las más conocidas distribuciones Linux existentes a nivel mundial, se basó en sus orígenes en Slackware. Entre las principales virtudes de esta distribución se encuentra el que sea una de las más sencillas de instalar y administrar, ya que cuenta con varios asistentes gráficos para completar diversas tareas en especial por su gran herramienta de instalación y configuración YaST.



- **Red Hat Enterprise Linux** también conocido por sus siglas RHEL es una distribución comercial de Linux desarrollada por Red Hat. Es la versión comercial basada en Fedora que a su vez está basada en el anterior Red Hat Linux.



Cada una de estas versiones cuenta con una serie de servicios de

valor añadido en base a los que basa su negocio (soporte, formación, consultoría, certificación, etc).

- **CentOS** (Community ENTERprise Operating System) es una bifurcación a nivel binario de la distribución Linux Red Hat Enterprise Linux RHEL, compilado por voluntarios a partir del código fuente liberado por Red Hat.

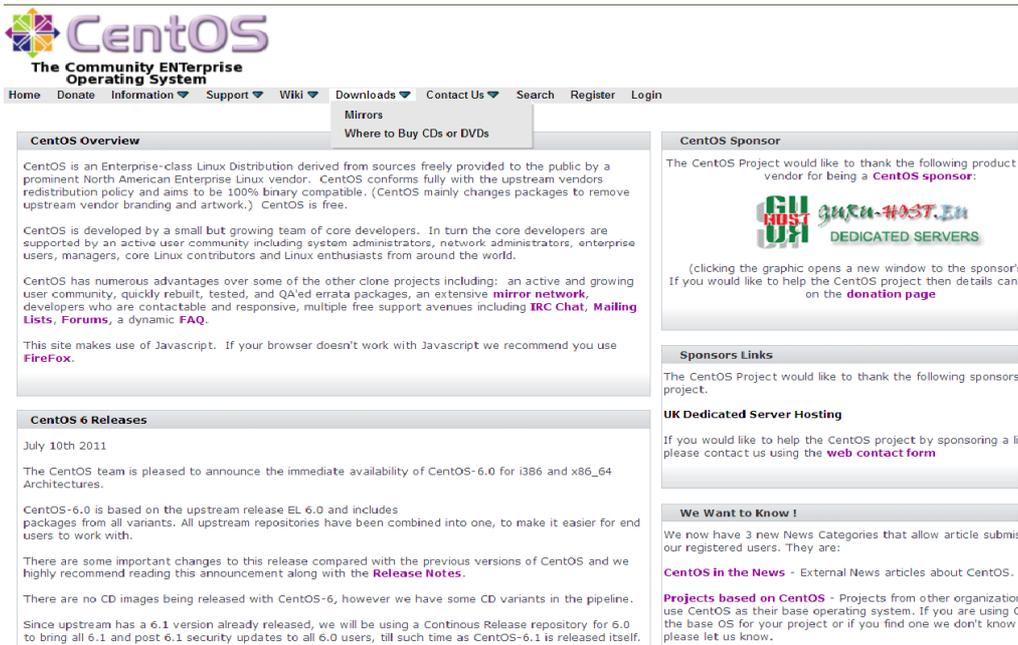


Red Hat Enterprise Linux se compone de software libre y código abierto, pero se publica en formato binario usable (CD-ROM o DVD-ROM) solamente a suscriptores pagados. Como es requerido, Red Hat libera todo el código fuente del producto de forma pública bajo los términos de la Licencia pública general de GNU y otras licencias. Los desarrolladores de CentOS usan ese código fuente para crear un producto final que es muy similar al Red Hat Enterprise Linux y está libremente disponible para ser bajado y usado por el público, pero no es mantenido ni asistido por Red Hat.

De esta lista se ha descartado Red Hat ya que no queremos gastar dinero en la instalación del sistema. Dentro de las que se han seleccionado, podemos mencionar a CentOS como la que más se acerca a las necesidades de la empresa. Además de contar con un gran periodo de mantenimiento de seguridad, el hecho de estar vinculado con Red Hat hace que exista mucha documentación al respecto y que si algún día se considerase migrar el sistema a una distribución Red Hat el impacto sería menor. Otra de las razones para escoger CentOS es que ya tenemos otro sistema instalado con CentOS por lo que el personal de la empresa ya está habituado a su manejo.

4.2.3 Instalación CentOS

Primero vamos a la página web del fabricante (<http://www.centos.org/>), nos bajamos la imagen y la grabamos en un cd.



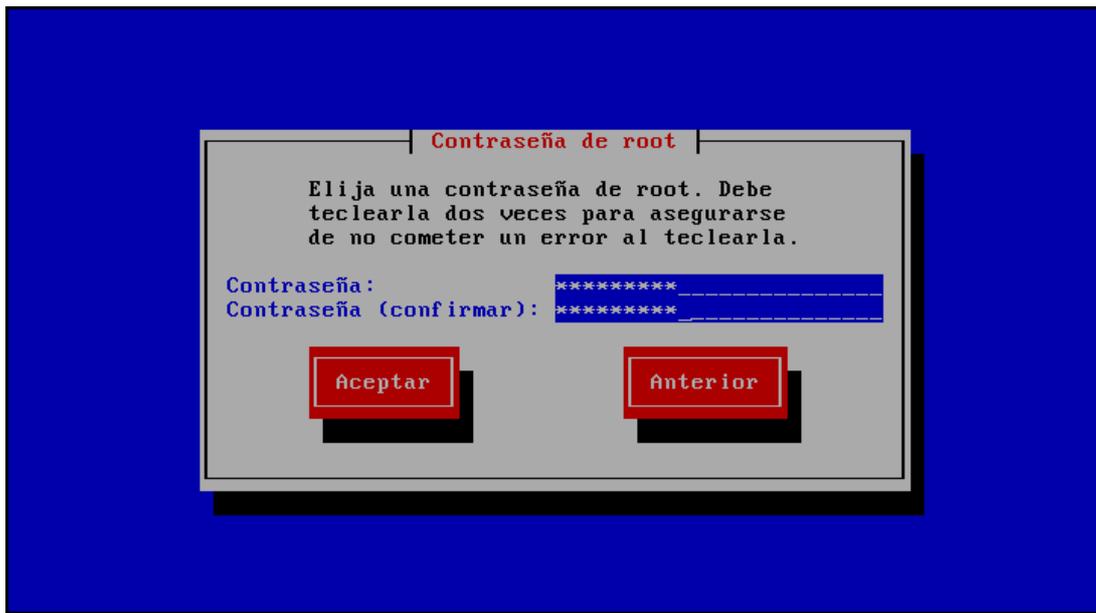
The screenshot shows the CentOS website homepage. At the top is the CentOS logo and the tagline "The Community Enterprise Operating System". Below the logo is a navigation menu with links for Home, Donate, Information, Support, Wiki, Downloads, Contact Us, Search, Register, and Login. The main content area is divided into several sections:

- CentOS Overview:** A section describing CentOS as an Enterprise-class Linux Distribution derived from sources freely provided to the public by a prominent North American Enterprise Linux vendor. It mentions that CentOS conforms fully with the upstream vendors redistribution policy and aims to be 100% binary compatible.
- CentOS 6 Releases:** A section dated July 10th 2011, announcing the immediate availability of CentOS-6.0 for i386 and x86_64 Architectures. It states that CentOS-6.0 is based on the upstream release EL 6.0 and includes packages from all variants.
- CentOS Sponsor:** A section thanking the following product vendor for being a CentOS sponsor, featuring a logo for "GURU-HOST.EU DEDICATED SERVERS".
- Sponsors Links:** A section thanking the following sponsors project.
- UK Dedicated Server Hosting:** A section inviting users to help the CentOS project by sponsoring a li, with a link to the web contact form.
- We Want to Know !:** A section mentioning 3 new News Categories that allow article submit our registered users.

Una vez hecho esto introducimos el CD en el servidor, lo encendemos y empezará la instalación del sistema operativo. Seleccionamos el idioma en el que queremos que sea instalado el sistema operativo.



Introducimos la contraseña de root.



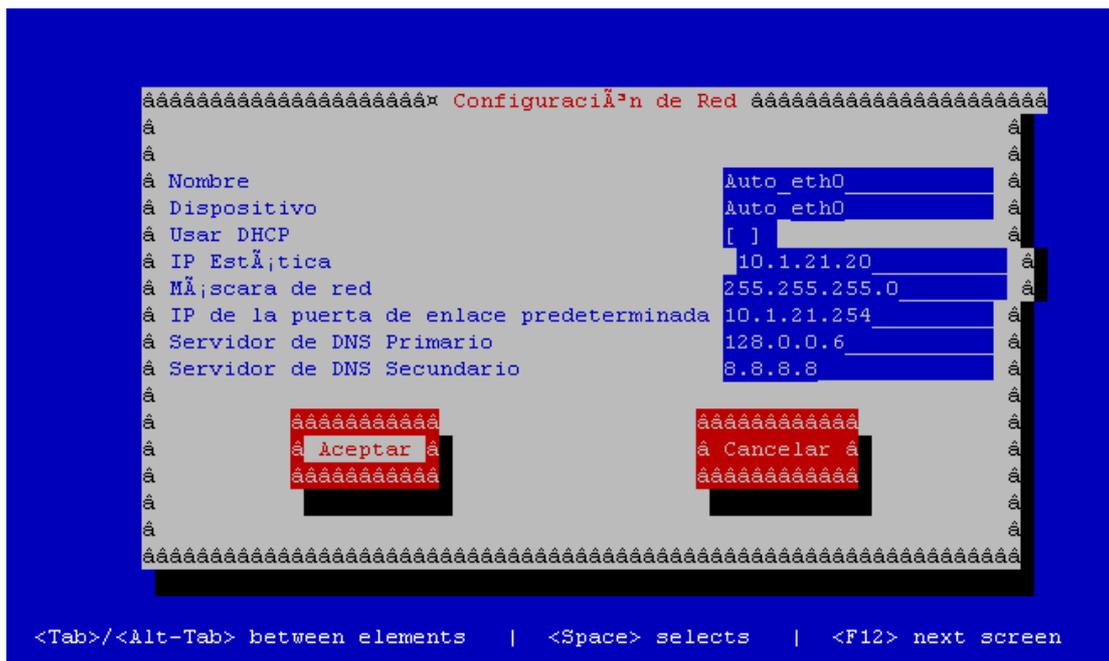
Y se iniciará el proceso de instalación del sistema operativo en el disco duro. Una vez finalizado nos pedirá reiniciar.



Una vez reiniciado debemos configurar una serie de parámetros:



Entramos en configuración de red para poner el servidor en nuestra red.



Una vez instalado todo correctamente vamos a preparar el sistema para poder instalar Asterisk. Primero pondremos en el fichero de configuración de yum nuestro Proxy para poder instalar los paquetes necesarios:

En `/etc/yum.conf` al final de `[main]` añadimos la línea:

proxy=http://yourproxyaddress:port/.

Una vez hecho esto instalamos los paquetes necesarios y sus dependencias:

```
yum groupinstall core
```

```
yum groupinstall base
```

```
yum install gcc gcc-c++ wget bison mysql-devel mysql-server php php-mysql php-pear php-pear-DB php-mbstring tftp-server httpd make ncurses-devel libtermcap-devel sendmail sendmail-cf caching-nameserver sox newt-devel libxml2-devel libtiff-devel php-gd audiofile-devel gtk2-devel subversion kernel-devel.
```

Es importante instalar el paquete php-pear-DB ya que no viene incluido. Tenemos que descargarlo desde el sitio oficial de redhat e instalarlo, de lo contrario FreePBX fallaría a la hora de instalarlo:

```
cd /usr/src
```

```
wget http://download.fedora.redhat.com/pub/epel/6/i386/php-pear-DB-1.7.13-3.el6.noarch.rpm
```

```
rpm -ivh php-pear-DB-1.7.13-3.el6.noarch.rpm
```

```
yum -y install php-process
```

El firewall (iptables) esta activado por defecto y su configuración bloquea la interfaz gráfica de FreePBX. Para que funcione correctamente ejecutaremos **system-config-firewall-tui** y configuraremos el firewall abriendo los siguientes puertos:

TCP 80 (www)

TCP 4445 (Flash Operator Panel)

UDP 5060-5061 (SIP)

UDP 10,000 - 20,000 (RTP)

UDP 4569 (IAX)

TCP 22 (SSH)

UDP 161 (snmp)

UDP 162 (snmp)

El servicio SELINUX no es recomendable dejarlo habilitado ya que da problemas con Asterisk, para deshabilitarlo editamos el fichero **/etc/selinux/config**, y ponemos el parámetro **SELINUX=disabled**.

Para que php funcione correctamente con FreePBX, debemos configurarle la zona horaria. Para ello debemos configurar el archivo **php.ini**:

vi +946 /etc/php.ini

Descomentar date.timezone y añadir **date.timezone=Europe/Madrid**

```
;;;;;;;;;;;;;;;;;;;;;;;;;
; Module Settings ;
;;;;;;;;;;;;;;;;;;;;;;;;;

[Date]
; Defines the default timezone used by the date functions
; http://www.php.net/manual/en/datetime.configuration.php#ini.date.timezone
date.timezone = Europe/Madrid
```

Una vez hecho esto reiniciamos apache para que se guarden los cambios:

service httpd restart

4.2.4 Instalación y configuración de Asterisk y FreePBX

Descargamos FreePBX y lo descomprimos:

cd /usr/src

wget http://mirror.freepbx.org/freepbx-2.9.0.tar.gz

tar zxvf freepbx-2.9.0.tar.gz

Descargamos Asterisk v1.8.

wget <http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-1.8-current.tar.gz>

```
[root@localhost src]# wget http://downloads.asterisk.org/pub/telephony/asterisk/
asterisk-1.8-current.tar.gz
--2011-11-02 18:32:09-- http://downloads.asterisk.org/pub/telephony/asterisk/as
terisk-1.8-current.tar.gz
Connecting to 128.254.254.2:80... conectado.
Petición Proxy enviada, esperando respuesta... 200 OK
Longitud: 28557326 (27M) [application/x-gzip]
Saving to: `asterisk-1.8-current.tar.gz'

94% [=====>] 1 27.012.334 344K/s eta 5s
```

tar zxvf asterisk-1.8-current.tar.gz

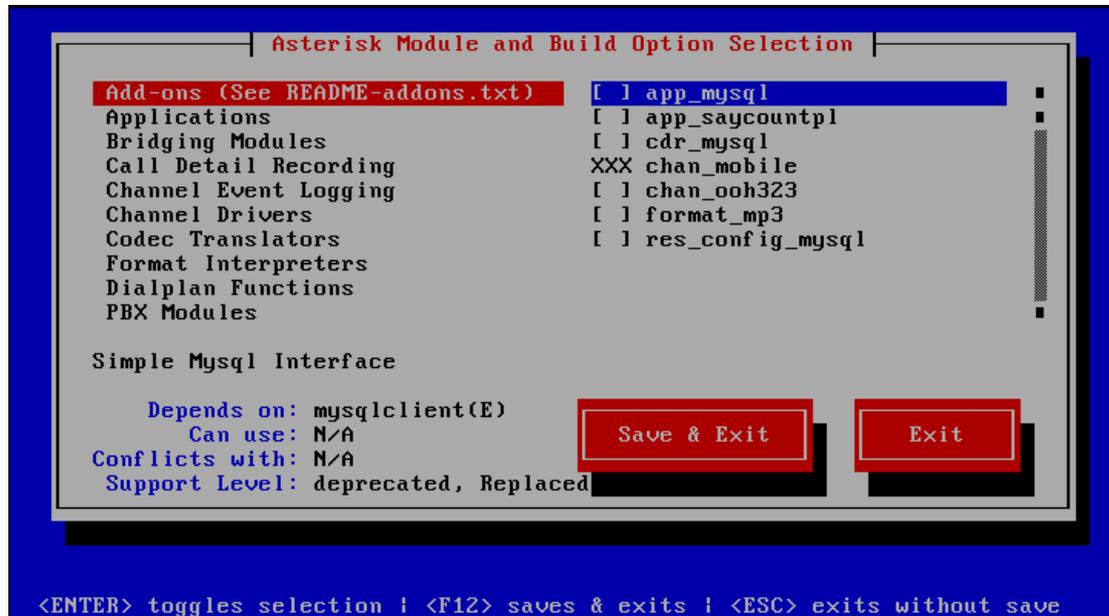
Configurar y compilar Asterisk (en nuestro caso la version actual era la 1.8.7.1):

cd /usr/src/asterisk-1.8.7.1

make clean

./configure && make menuselect

Con menuselect llegaremos a la siguiente pantalla:



De add-ons seleccionamos todos excepto “format_mp3”. Seleccionamos ulaw como sonido mejor que gsm para poder conectar más tarde correctamente con el Call Manager de Cisco. Una vez hecho esto asegurarse de que guardamos.

Por último instalamos Asterisk: **make && make install && make samples**

Crearemos un usuario de Asterix:

useradd -c “Asterisk PBX” -d /var/lib/asterix Asterix

Y hacemos a dicho usuario propietario.

chown -R asterisk /var/run/asterisk

chown -R asterisk /var/log/asterisk

chown -R asterisk /var/lib/asterisk/moh

chown -R asterisk /var/lib/php/session

También cambiaremos el usuario apache y el grupo apache a usuario Asterix y grupo Asterisk:

sed -i "s/User apache/User asterisk/" /etc/httpd/conf/httpd.conf

sed -i "s/Group apache/Group asterisk/" /etc/httpd/conf/httpd.conf

4.2.5 Configuración MySQL

Antes de empezar tenemos que asegurarnos que MySQL esta arrancado:

```
service mysqld start
```

Ahora configuramos las bases de datos para FreePBX:

```
cd /usr/src/freepbx-2.9.0
```

```
mysqladmin create asterisk
```

```
mysqladmin create asteriskcdrdb
```

```
mysql asterisk < SQL/newinstall.sql
```

```
mysql asteriskcdrdb < SQL/cdr_mysql_table.sql
```

Estas bases de datos necesitan ser seguras y FreePBX pedirá por un usuario y una contraseña, nosotros pondremos como usuario “asteriskuser” y como contraseña “amp109” para ello:

```
mysql
```

```
mysql> GRANT ALL PRIVILEGES ON asteriskcdrdb.* TO  
asteriskuser@localhost IDENTIFIED BY 'amp109';
```

```
Query OK, 0 rows affected (0.00 sec)
```

```
mysql> GRANT ALL PRIVILEGES ON asterisk.* TO asteriskuser@localhost  
IDENTIFIED BY 'amp109';
```

```
Query OK, 0 rows affected (0.00 sec)
```

```
mysql> flush privileges;
```

```
Query OK, 0 rows affected (0.00 sec)
```

```
mysql> \q
```

```
Bye
```

Para acabar, debemos poner un password de root a mysql. Como ejemplo pondremos como password “abcdef”

```
mysqladmin -u root password 'abcdef'
```

Ahora aumentaremos el rendimiento de MySQL. Abriremos el fichero my.cnf y añadiremos skip-innodb. Y hecho esto aumentamos la seguridad previniendo que IPs

externas puedan conectarse al puerto de MySQL, para eso en el mismo fichero añadiremos la línea **bind-address = 127.0.0.1**.

vi /etc/my.cnf

El archivo debe quedar:

```
[mysqld]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
user=mysql
skip-innodb
bind-address = 127.0.0.1
# Disabling symbolic-links is recommended to prevent assorted security risks
symbolic-links=0

[mysqld_safe]
log-error=/var/log/mysqld.log
pid-file=/var/run/mysqld/mysqld.pid
```

Hecho esto escribimos por consola:

service mysqld restart

4.2.6 Instalación de FreePBX

/usr/sbin/safe_asterisk

cd /usr/src/freepbx-2.9.0

./install_amp --username=asteriskuser --password=amp109

Al hacer este paso es normal que de una serie de warnings. Son warnings que nos indican que actualicemos los módulos de Asterisk y FreePBX por el explorador.

El usuario por defecto de FreePBX: admin y el password: admin. Este password lo podemos cambiar después por el explorador.

Editaremos el archivo **/etc/asterisk/cdr_mysql.conf** y añadiremos **loguniqueid=yes** en la sección global. Con esto conseguiremos que cada registro de llamada tenga un identificador numérico único.

vi /etc/asterisk/cdr_mysql.conf

Y ahora hacemos que FreePBX se ejecute al iniciarse CentOS:

echo /usr/local/sbin/ampportal start >> /etc/rc.local

También haremos que Apache y MySQL se ejecuten al inicio:

chkconfig httpd on

chkconfig mysqld on

Ahora reiniciamos CentOS y al iniciar podremos acceder a FreePBX desde un explorador. Lo primero que tenemos que hacer al entrar la primera vez en FreePBX es apretar en “Apply Configuration Changes” así todos los .conf se crearán y después vamos a CentOS y escribimos **amportal restart** para así reiniciar FreePBX.

4.2.7 Configuración inicial de FreePBX

Abriremos un explorador y escribiremos:

<http://10.1.21.20>

Y veremos una página similar a esta:



Clickamos en FreePBX Administration y nos pedirá usuario y contraseña. Como todavía no hemos configurado nada por defecto es User:admin, Password:admin.

Y nos encontraremos con el panel de estado del sistema de FreePBX:

The screenshot displays the FreePBX System Status page. At the top, it shows the FreePBX logo and version (2.9.0.7 on 10.1.21.20). The navigation menu includes Admin, Reports, Panel, Recordings, and Help. The main content area is divided into several sections:

- FreePBX Notices:** Contains three notices, including a warning about a failed symlink and a note about the default Asterisk Manager Password.
- FreePBX Statistics:** Shows call and channel statistics, such as Total active calls (0) and Total active channels (0).
- FreePBX Connections:** Displays active connections for Phones (2) and Trunks (2).
- Uptime:** Shows System Uptime (1 week, 1 hour, 5 minutes) and Asterisk Uptime (4 hours, 23 minutes).
- System Statistics:** Provides detailed system metrics for Processor (Load Average: 0.80), Memory (Used: 27%), Disks (Used: 8%), and Networks (eth0 receive/transmit, eth1 receive/transmit).
- Server Status:** Lists the status of Asterisk, Op Panel, MySQL, Web Server, and SSH Server, all showing as OK.

Lo primero que haremos es cambiar la contraseña para entrar a administrar FreePBX, para ello vamos a: **Tools>Advanced Administration>Advanced Settings>System Setup>User Portal Admin Password.**

También cambiaremos el password para acceder a Voicemail & Recordings (ARI): **System Setup>FreePBX Web Address.**

De nuevo una vez hecho esto clickamos en **Apply Configuration Changes.**

4.2.8 Rotación de logs

Es interesante hacer una rotación de los logs ya que sino en poco tiempo se crean archivos de log muy grandes. Para ello creamos el siguiente archivo:

```
vi /etc/logrotate.d/asterisk
```

Y dentro añadimos lo siguiente, de esta forma conseguiremos que los logs de Asterisk rotaran semanalmente, el archivo tiene que quedar:

```

/var/log/asterisk/messages /var/log/asterisk/*log /var/log/asterisk/full {
missingok
notifempty
sharedscripts
create 0640 asterisk asterisk
postrotate
/usr/sbin/asterisk -rx 'logger reload' > /dev/null 2> /dev/null
endscript
}

```

4.2.9 Administración de FreePBX

Cuando entramos en el panel de administración de FreePBX, en la primera pantalla vemos lo siguiente:

The screenshot displays the FreePBX System Status dashboard. At the top, the FreePBX logo is visible along with navigation tabs for Admin, Reports, Panel, Recordings, and Help. The main content area is divided into several sections:

- FreePBX Notices:** Shows two warnings: "SymLink from modules failed" and "Default Asterisk Manager Password Used".
- FreePBX Statistics:** Displays real-time metrics:

Telnet active calls	1
Internal calls	0
External calls	0
Telnet active channels	1
- FreePBX Connections:** Shows the status of IP Phones (3 Online) and IP Trunks (1 Online).
- Uptime:** Reports System Uptime and Asterisk Uptime as 1 hour, 14 minutes, with a Last Reload of 9 minutes.
- System Statistics:** Provides a detailed overview of system resources:

Processor	
Load Average	0.00
CPU	0%
Memory	
Free Memory	9%
Swap	0%
Disks	
/dev/shm	0%
/boot	11%
/home	1%
Networks	
eth0 receive	0.00 KB/s
eth0 transmit	0.00 KB/s
eth1 receive	0.00 KB/s
eth1 transmit	0.00 KB/s
- Server Status:** A summary of critical services:

Asterisk	OK
OS Panel	OK
MySQL	OK
Web Server	OK
SSH Server	OK

The left sidebar contains a comprehensive menu for system administration, including Setup, Tools, Admin, and various modules like Extensions, Feature Codes, and Inbound Call Control.

En la parte derecha de la misma vemos el nivel de carga de la CPU, la memoria y la cantidad de disco ocupado en tiempo real.

También podemos ver el estado de todos los servicios del servidor imprescindibles para que Asterisk funcione.

En la parte central, vemos el total de llamadas activas que se están realizando en este momento, así como la cantidad de canales que se están utilizando. Más abajo podemos ver los teléfonos que tenemos conectados a Asterisk así como la cantidad de trunks conectados activos.

En la parte izquierda podemos ver las opciones de configuración de FreePBX.

Lo primero que tenemos que hacer es cambiar la contraseña por defecto para administrar FreePBX para ello vamos al archivo **amportal.conf**:

vi /etc/amportal.conf

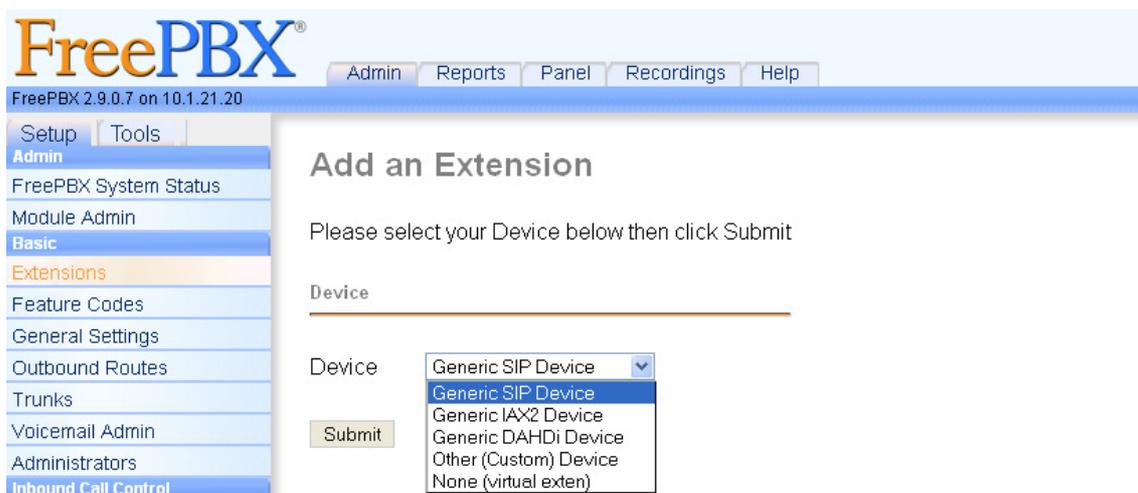
Buscamos la línea que pone **AMPMGRUSER=admin**. Y añadimos debajo de esta línea:

AMPMGRPASS=secret123password (donde secret123password es el password que queremos poner para entrar a administrar con FreePBX).

4.3 Configuración de Asterisk mediante FreePBX

4.3.1 Configuración de las extensiones

Para configurar una extensión vamos a **Setup > Extensions**. Una vez allí vemos que podemos elegir entre 5 tipos de dispositivos.



Elegiremos la opción de dispositivo SIP. Una vez apretemos “Submit” nos aparecerá la pantalla para configurar las características de la extensión.

En dicha pantalla tenemos que escribir el número de extensión y el nombre de extensión que queremos configurar. Todas las demás configuraciones las dejaremos por defecto.

The screenshot shows the FreePBX 2.9.0.7 web interface. The top navigation bar includes 'Admin', 'Reports', 'Panel', 'Recordings', and 'Help'. The sidebar menu on the left lists various configuration categories: Setup, Tools, Admin, FreePBX System Status, Module Admin, Basic, Extensions (highlighted), Feature Codes, General Settings, Outbound Routes, Trunks, Voicemail Admin, Administrators, Inbound Call Control (highlighted), Inbound Routes, Zap Channel DIDs, Announcements, Blacklist, Call Flow Control, CallerID Lookup Sources, Directory, Follow Me, IVR, Queues, Ring Groups, Time Conditions, Time Groups, Internal Options & Configuration (highlighted), Conferences, and Music on Hold.

Add SIP Extension

Add Extension

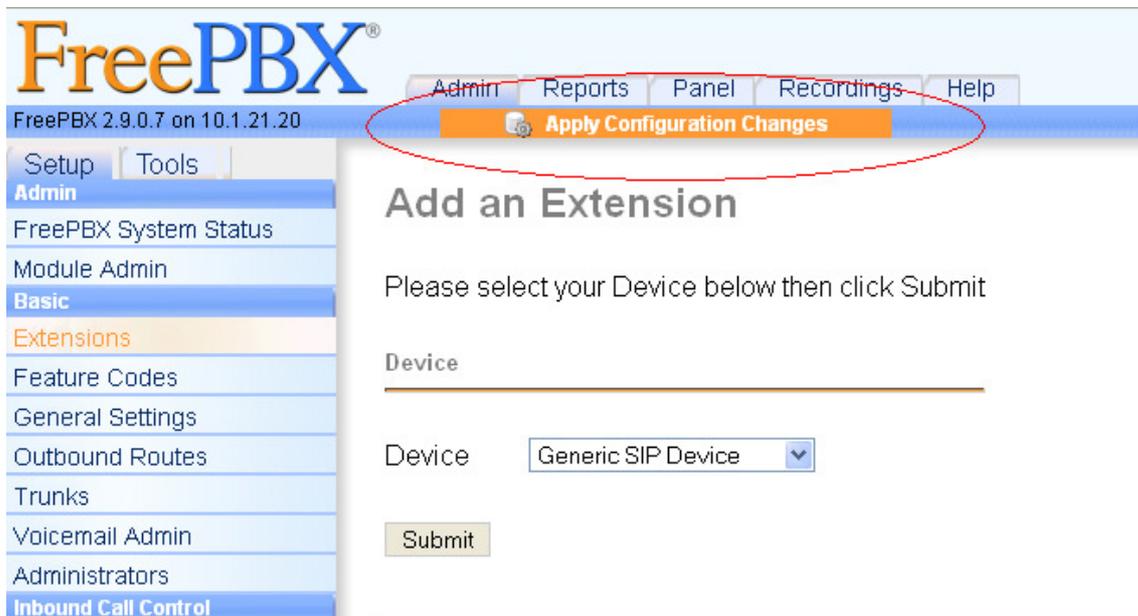
User Extension	<input type="text" value="8000"/>
Display Name	<input type="text" value="Centralita"/>
CID Num Alias	<input type="text"/>
SIP Alias	<input type="text"/>

Extension Options

Outbound CID	<input type="text"/>
Ring Time	<input type="text" value="Default"/>
Call Forward Ring Time	<input type="text" value="Default"/>
Outbound Concurrency Limit	<input type="text" value="No Limit"/>
Call Waiting	<input type="text" value="Enable"/>
Internal Auto Answer	<input type="text" value="Disable"/>
Call Screening	<input type="text" value="Disable"/>
Pinless Dialing	<input type="text" value="Disable"/>
Emergency CID	<input type="text"/>
Queue State Detection	<input type="text" value="Use State"/>

Assigned DID/CID

Una vez clickemos en **Submit** nos volverá a la pantalla principal de extensiones que tenemos y nos aparecerá **Apply Configuration Changes**. Apretamos para que la extensión se grabe en los ficheros de configuración de Asterisk.



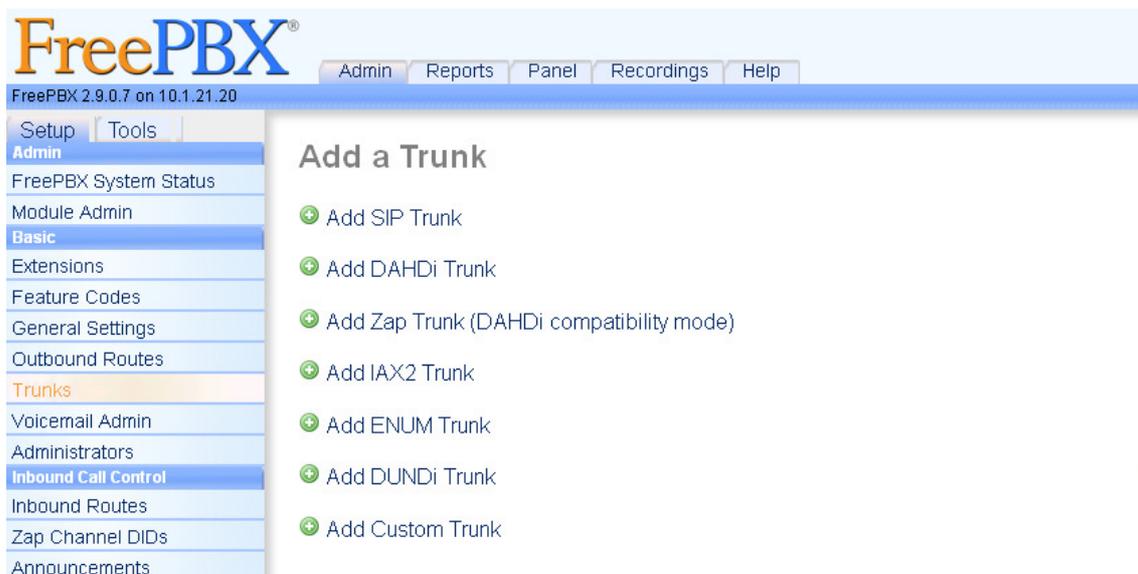
Cuando hayamos hecho esto nos aparecerán las extensiones configuradas a la derecha.



4.3.2 Configuración de los troncales (Trunks)

Los troncales se utilizan para conectar diferentes centralitas y así poder realizar llamadas entre extensiones configuradas en cada una de ellas.

Como podemos ver podemos configurar 7 tipos de trunks.



En nuestro caso configuraremos trunks SIP ya que es la única forma de poder conectar Asterisk con Cisco Call Manager.

Para ello seleccionamos Add SIP Trunk y nos llevará a la página de configuración del trunk.

Los parámetros a configurar son:

- **type = peer.** Utilizamos peer ya que todo lo que pase será enviado a una entidad SIP a la cual Asterisk enviará llamadas.
- **qualify = yes.** Con esta opción activada Asterisk comprueba regularmente el estado del teléfono y comprueba que este activo.
- **nat = no.** Como no hay nat para llegar de un lado al otro del trunk desactivamos el nat.
- **insecure = very.** Con esta opción configuramos que no haya autenticación de usuario/password para comunicar en el trunk.

- **host = ip.** En esta opción configuramos la ip del Call Manager con el que queremos conectar.
- **dtmf=rfc2833.** Esta opción es la señalización requerida entre ambas centralitas.
- **disallow = all.** Se desactivan todos los codecs para el trunk, esta acción se realiza porque para activar un codec primero se tienen que desactivar todos los codecs.
- **context=from-internal.** El contexto en el que una extensión se encuentra define las características y los trunks a los que podrá acceder. Por defecto Asterisk deja todos los usuarios en el contexto from-internal, es por eso que definimos que ese contexto pueda realizar llamadas a través de ese trunk para que todas las extensiones puedan llamar.
- **careinvite=no.** Con el careinvite configurado a no, una vez establecida la llamada Asterisk deja de enviar paquetes INVITES. Como una vez establecida la llamada no necesitamos más INVITES para que no se sature la línea denegamos esta opción.
- **allow=ulaw.** Con esta opción activamos el codec ulaw . Este codec es el G.711, el cual utiliza 64kbps para cada lado de la llamada.

En nuestro caso tenemos el trunk que conecta con el Call Manager de Barcelona y la configuración debe quedar de la siguiente forma:

Edit SIP Trunk

⊖ Delete Trunk CCMTrunkBcn

In use by 1 route

General Settings

Trunk Name:

Outbound CallerID:

CID Options: ▼

Maximum Channels:

Disable Trunk: Disable

Monitor Trunk Failures: Enable

Outgoing Settings

Trunk Name:

PEER Details:

```
type=peer
qualify=yes
nat=no
insecure=very
host=10.1.0.20
dtmf=rfc2833
disallow=all
context=from-internal
canreinvite=no
allow=ulaw
```

Incoming Settings

USER Context:

USER Details:

```
type=peer
qualify=yes
nat=no
insecure=very
host=10.1.0.20
dtmf=rfc2833
disallow=all
context=from-internal
canreinvite=no
allow=ulaw
```

Registration

Register String:

Y el trunk que conecta con el Call Manager de Madrid:

Edit SIP Trunk

 Delete Trunk CCMTrunkMadrid

In use by 1 route

General Settings

Trunk Name:

Outbound CallerID:

CID Options:

Maximum Channels:

Disable Trunk: Disable

Monitor Trunk Failures: Enable

Outgoing Settings

Trunk Name:

PEER Details:

```
type=peer
qualify=yes
nat=no
insecure=very
host=10.1.85.20
dtmf=rfc2833
disallow=all
context=from-internal
canreinvite=no
allow=ulaw
```

Incoming Settings

USER Context:

USER Details:

```
type=peer
qualify=yes
nat=no
insecure=very
host=10.1.85.20
dtmf=rfc2833
disallow=all
context=from-internal
canreinvite=no
allow=ulaw
```

Registration

Register String:

4.3.3 Configuración de las llamadas salientes (Outbound Routes)

Para poder realizar llamadas a extensiones configuradas en el Call Manager de Cisco tenemos que indicarle a Asterisk que dichas extensiones y prefijos los enrute por el trunk hacia el Call Manager de Cisco, es decir, la llamadas externas se envían a través del trunk como se determina en la configuración del Outbound Routes.

Para configurar la ruta de salida vamos a **Setup > Outbound Routes**.

Una vez allí tenemos que configurar:

- **Route Name:** nombre que le queremos dar a las rutas que estemos configurando.
- **Route Password:** si ponemos un número como contraseña, cuando el que realiza la llamada llama a un número que coincide con alguno de los patrones asignados se le pide un número de contraseña para poder llamar.
- **Dial Patterns:** el Dial Pattern es un conjunto de dígitos que si la llamada se realiza a un número que coincide con alguno de estos patrones, esa llamada será enrutada por el trunk.

Hay que configurar un Dial Pattern por línea. Para configurar un patrón hay unas reglas:

- X – coincide cualquier dígito entre 0-9
 - Z – coincide cualquier dígito entre 1-9
 - N – coincide cualquier dígito entre 2-9
 - [1237 - 9] – coincide cualquier dígito que se encuentre
 - . – se utiliza para separar el prefijo
- **Trunk Sequence:** aquí hay que configurar en el orden en que queremos que se elijan los trunks una vez han coincidido los Dial Patterns antes configurados. En nuestro caso primero elegiremos el trunk de Barcelona y después el trunk de Madrid.

En nuestro caso tenemos configurados dos Outbound Routes. Uno para móviles el cual te pide contraseña y otro para llamadas nacionales y a extensiones de Cisco.

Ambas quedan configuradas de la siguiente manera:

Route Settings

Route Name:
Route CID: Override Extension
Route Password:
Route Type: Emergency Intra-Company
Music On Hold?:
Time Group:
Route Position:
Additional Settings

PIN Set:

Dial Patterns that will use this Route

<input type="text" value="(prepend) + prefix [0.0XX"/>	<input type="text" value="/ CallerID"/>	<input type="button" value="🗑"/>
<input type="text" value="(prepend) + prefix [0.[8-9]0[0-2]XXXXXX"/>	<input type="text" value="/ CallerID"/>	<input type="button" value="🗑"/>
<input type="text" value="(prepend) + prefix [0.[8-9]XXXXXXXX"/>	<input type="text" value="/ CallerID"/>	<input type="button" value="🗑"/>
<input type="text" value="(prepend) + prefix [XXXX"/>	<input type="text" value="/ CallerID"/>	<input type="button" value="🗑"/>
<input type="text" value="(prepend) + prefix [match pattern"/>	<input type="text" value="/ CallerID"/>	<input type="button" value="🗑"/>

Dial patterns wizards:

Trunk Sequence for Matched Routes

0	<input type="text" value="CCMTrunkBcn"/>	<input type="button" value="🗑"/>	<input type="button" value="▼"/>
1	<input type="text" value="CCMTrunkMadrid"/>	<input type="button" value="🗑"/>	<input type="button" value="▲"/>
2	<input type="text"/>		<input type="button" value="▼"/>

Route Settings

Route Name:
Route CID: Override Extension
Route Password:
Route Type: Emergency Intra-Company
Music On Hold?:
Time Group:
Route Position:
Additional Settings

PIN Set:

Dial Patterns that will use this Route

<input type="text" value="(prepend)"/>	+	<input type="text" value="prefix"/>		<input type="text" value="[0.[6-7]XXXXXXXX"/>	/	<input type="text" value="CallerID"/>	<input type="button" value=""/>
<input type="text" value="(prepend)"/>	+	<input type="text" value="prefix"/>		<input type="text" value="[6XXXX"/>	/	<input type="text" value="CallerID"/>	<input type="button" value=""/>
<input type="text" value="(prepend)"/>	+	<input type="text" value="prefix"/>		<input type="text" value="[match pattern"/>	/	<input type="text" value="CallerID"/>	<input type="button" value=""/>

+ Add More Dial Pattern Fields

Dial patterns wizards:

Trunk Sequence for Matched Routes

0
1
2

Add Trunk

Submit Changes

Duplicate Route

4.3.4 Configuración de Inbound Routes

En la página de Inbound Routes podemos configurar el destino que utiliza Asterisk para las llamadas entrantes desde los troncales. Cuando se recibe una llamada desde algún troncal, se identifican el DID (numero marcado por el llamante) y el CID (número desde el cual se realiza la llamada) y la llamada se deriva según la configuración.

Para configurarlo:

- **Número de DID:** Para una extensión SIP o IAX2, el número DID es normalmente el número de cuenta.
- **Número de Caller ID:** Este es el número de identificador de llamadas del servidor del proveedor.

Si dejamos estas dos casillas en blanco se reconocerán todas las llamadas entrantes sin restricciones.

- **Set Destination:** Aquí seleccionamos a quien será direccionada la llamada entrante. Entre otras opciones la podemos derivar a un grupo de extensiones, a una extensión, a un IVR, terminar la llamada o hacia un trunk.

Add Incoming Route

Add Incoming Route

Description:
DID Number:
CallerID Number:
CID Priority Route:

Options

Alert Info:
CID name prefix:
Music On Hold:
Signal RINGING:
Pause Before Answer:

Privacy

Privacy Manager:

CID Lookup Source

== choose one ==
Directory
Extensions
Feature Code Admin
IVR
Ring Groups
Terminate Call
Trunks

== choose one ==

4.3.5 Configuración Follow Me

Esta opción nos permite transferir una llamada a otra extensión o a un grupo de extensiones en caso de no encontrarse dicha extensión disponible. En el caso que nadie del grupo conteste podemos incluso ejecutar el Voicemail.

Para configurarlo vamos a **Setup > Follow Me**



Aquí podemos ver todas las extensiones que tenemos configuradas en Asterisk. Clickamos en la extensión que queremos hacer “follow me” si nadie contesta a esa extensión. Una vez clickado pasamos a la página de configuración. En esta página tenemos que configurar:

- **Initial Ring Time**, que es el tiempo que sonará el primer teléfono del grupo antes de pasar la llamada al siguiente.
- El **Ring Time** tiempo en segundos que sonará cada teléfono antes de pasar al siguiente.
- **Follow-Me List** la lista de extensiones que están en el grupo de salto.
- **Destination if no answer** editaremos lo que queremos hacer si nadie del grupo contesta a la llamada. En nuestro caso hemos elegido terminar la llamada.

Follow Me: 8001

 Edit Extension 8001

Delete Entries

Edit Follow Me

Disable:

Initial Ring Time:

Ring Strategy:

Ring Time (max 60 sec):

Follow-Me List:

Extension Quick Pick:

Announcement:

Play Music On Hold?:

CID Name Prefix:

Alert Info:

Call Confirmation Configuration

Confirm Calls:

Remote Announce:

Too-Late Announce:

Change External CID Configuration

Mode:

Fixed CID Value:

Destination if no answer:

Terminate Call:

4.3.6 Configuración Ring Groups

La configuración de un Ring Group nos da la posibilidad de crear una extensión “virtual” con la que poder llamar a un grupo concreto de extensiones. Para ello como ejemplo crearemos el Ring Group de Informatica con la extensión 8099. Si llamamos a dicha extensión primero sonará la extensión 8003, si esta ocupada o no se coge el teléfono, la llamada pasará a la extensión 8001 y si pasa igual lo mismo se pasará la llamada a la 8002. De igual forma que antes si nadie contesta dicha llamada se colgará.

Para configurarla vamos a **Setup > Ring Groups**.

Una vez allí tenemos que configurar:

- **Group Description:** nombre que le queremos dar al grupo de llamada
- **Ring Strategy:** aquí elegiremos cómo queremos que suenen las extensiones configuradas dentro del grupo. Así si elegimos **ringall** al llamar al número configurado para el grupo sonarán todas las extensiones configuradas a la vez. Si elegimos **hunt** sonarán las extensiones en el orden que estén configuradas en el apartado **Extension List**.
- **Ring Time:** es el tiempo que queremos que suenen los teléfonos a la vez antes de que pasemos la llamada a la condición **Destination if no answer**, o si tenemos configurada la Ring Strategy en modo hunt el tiempo que queremos que suene un teléfono antes de que pase al siguiente teléfono.

Ring Group: 8099

Delete Group

Edit Ring Group

Group Description:	Informatica
Ring Strategy:	ringall
Ring Time (max 60 sec)	20
Extension List:	8003 8001 8002
Extension Quick Pick	(pick extension)
Announcement:	None
Play Music On Hold?	Ring
CID Name Prefix:	
Alert Info:	
Ignore CF Settings:	<input type="checkbox"/>
Skip Busy Agent:	<input checked="" type="checkbox"/>
Enable Call Pickup:	<input type="checkbox"/>
Confirm Calls:	<input type="checkbox"/>
Remote Announce:	Default
Too-Late Announce:	Default

Change External CID Configuration

Mode:	Default
Fixed CID Value:	

Destination if no answer:

Terminate Call	Hangup
----------------	--------

- **Extension List:** aquí agregamos las extensiones que queremos que estén en el grupo.
- **Skip Busy Agent:** si marcamos esta opción saltará a la siguiente extensión en la lista si dicha extensión esta ocupada.
- **Destination if no answer:** esta opción configura el comportamiento que debe hacer Asterisk si nadie a cogido el teléfono. Hay muchas opciones, como terminar la llamada y colgar, o dar comunicando, o pasar a otra extensión, etc.

4.3.7 Otros servicios de Asterisk

4.3.7.1 IVR (Interactive Voice Responce)

El IVR es una recepcionista digital, podemos configurar mensajes grabados por nosotros o mensajes que ya tiene Asterisk por defecto.

Para utilizarlo hay que grabar los mensajes que irá escuchando la persona que llame y añadir dichas locuciones a las teclas que marcará para realizar las diferentes acciones.

Para poder utilizar grabaciones hechas por nosotros, estas grabaciones tienen que estar grabadas y configuradas en la opción **System Recordings**.

Para configurar una recepcionista digital tenemos que ir a **Setup > IVR**. Una vez allí configurar:

- **Change Name:** aquí se configura el nombre que queremos dar a la recpcionista digital.
- **Announcement:** elegimos la grabación que queremos de bienvenida. Como hemos explicado anteriormente la grabación tiene que estar configurada en la sección de System Recording.
- **Direct Dial Options:** elegimos si la persona que llama puede introducir directamente la extensión a la que quiere llamar.
- Por último en la última sección configuraremos las teclas a presionar para ir a un lugar u otro. En el recuadro de la izquierda ponemos el dígito a apretar y en el desplegable lo que queramos que realice dicha tecla.

Por ejemplo la centralita de bienvenida queda:

Edit Menu Bienvenida

Change Name:
Announcement:
Timeout:
VM Return to IVR:
Direct Dial Options:
Loop Before t-dest:
Timeout Message:
Loop Before i-dest:
Invalid Message:
Repeat Loops:

<input type="text" value="1"/>	<input type="text" value="Extensions"/>	<input type="text" value="<8004> Toxico"/>	<input type="text" value="Return to IVR"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text" value="2"/>	<input type="text" value="Extensions"/>	<input type="text" value="<8005> Distribucion"/>	<input type="text" value="Return to IVR"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text" value="3"/>	<input type="text" value="Extensions"/>	<input type="text" value="<8006> Sistemas"/>	<input type="text" value="Return to IVR"/>	<input type="checkbox"/>	<input type="checkbox"/>

4.3.7.2 Blacklist

En la blacklist podemos ir añadiendo las extensiones que queremos bloquear. Es tan sencillo como escribir el número de extensión que queremos bloquear en **Number** y clicar **Submit Changes**.

Add or replace entry

Number:
Description:
Block Unknown/Blocked Caller ID:

4.3.7.3 Queues

Las colas permiten administrar un gran número de llamadas entrantes. Podemos configurar una gran variedad de opciones, como el tiempo de espera, la locución de espera o la música de espera.

En nuestro caso utilizaremos las colas para la extensión de Centralita, ya que mientras esta atendiendo una llamada muchas veces llamará otra persona y no queremos que al cliente le suene comunicando y perder la llamada.

En el menú izquierdo vamos a **Setup > Queues** y configuramos:

- **Queue number:** número que queremos que tenga la cola.
- **Queue name:** nombre que queremos dar a la cola.
- **Static agents:** ponemos las extensiones que asumimos que siempre van a estar en la cola.
- **IVR Break Out Menu:** si no se coge la llamada aparecerá una locución cada cierto periodo de tiempo que dice: nuestras líneas están ocupadas, un momento por favor.
- **Fail Over Destination – Queues:** elegiremos la opción ColaCentralita. Las llamadas quedarán siempre en cola hasta que se coja la llamada o el propio llamante cuelgue.

Las demás opciones las dejaremos por defecto.

4.3.7.4 Time Group y Time Conditions

Con estas opciones se puede configurar Asterisk para que actúe de una forma u otro dependiendo de la fecha o la hora en la cual se esta llamando. De esta forma si se llama un domingo y no se trabaja en domingo se puede conectar una locución que informe del horario de recepción de llamadas o por ejemplo también desviar la llamada a una extensión, de guardia que sí trabaja dicho día.

Para poder configurar esta opción primero tenemos que configurar un Time Group. Para configurar el time Group vamos a **Setup > Time Group**. Una vez allí tenemos que ponerle un nombre descriptivo a dicho grupo y configurar hora, día de la semana, día del mes o mes tanto de inicio como de final del tiempo que queremos configurar.

Una vez configurado el Time Group, vamos a **Setup > Time Conditions** introducimos un nombre descriptivo, seleccionamos el grupo creado previamente para que se cumpla esa condición de tiempo y entonces elegimos que acción realizar en caso de que la condición del grupo de tiempo coincida y la acción a realizar en caso de que no coincida. En el ejemplo de la captura de pantalla, hemos puesto que en caso que coincida que es domingo nos salte una locución previamente grabada informando del horario de atención al público. Y si coincide que la llamada no esta siendo realizada en domingo, la llamada nos vaya directamente a la centralita de la empresa.

Add Time Group

Time Group

Description: Domingo

New Time

Time to start: 00:00
Time to finish: 23:59
Week Day start: Sunday
Week Day finish: Sunday
Month Day start: -
Month Day finish: -
Month start: -
Month finish: -

Submit

Add Time Condition

Add Time Condition

Time Condition name: Domingo
Enable Override Code:
Time Group: Domingo

Destination if time matches:

IVR: Unnamed

Destination if time does not match:

Extensions: <8000> Centralita

Submit

4.3.7.5 Conferences

Con esta opción se puede configurar un número al que las extensiones llaman y así poder mantener una conversación todos juntos. En esta opción también se puede configurar un PIN necesario para entrar en la conferencia.

4.3.7.6 Music on Hold (Música en espera)

En esta sección se pueden configurar las diferentes canciones de música en espera. Podemos utilizar las que vienen por defecto con Asterisk o podemos subir nosotros mismos archivos en formato mp3 o wav.

Podemos hacer diferentes categorías de músicas dependiendo si las queremos para las colas o para la música que suena cuando dejamos en espera a la persona que llama.

4.3.7.7 System Recording

Aquí grabamos las locuciones o mensajes que queremos utilizar en el IVR o en cualquier otra sección.

Para cargar dichos mensajes tenemos dos opciones:

- Desde teléfono IP: Ponemos la extensión desde la que queremos grabar la locución y una vez queremos grabarla marcamos *77 en dicho teléfono y al escuchar la señal grabamos la locución. Una vez hemos grabado, podemos comprobar la grabación marcando *99 en el mismo teléfono. Si estamos conformes con la grabación le ponemos un nombre y le damos a guardar.
- Desde una aplicación de grabación de sonido en el ordenador: Podemos utilizar la utilidad predeterminada de Windows o de cualquier sistema operativo y con un micrófono grabar la locución. Una vez hecho esto guardarla en formato PCM Encoded, 16 Bits, at 8000Hz, tal y como se pide y poner la ruta de dicho archivo dentro de FreePBX para subir la locución a Asterisk.

System Recordings English

Add Recording Add Recording Built-in Recordings

Step 1: Record or upload

Using your phone, dial *77 and speak the message you wish to record.

Alternatively, upload a recording in any supported asterisk format. Note that if you're using .wav, (eg, recorded with Microsoft Recorder) the file **must** be PCM Encoded, 16 Bits, at 8000Hz.

Examine... Upload

Step 2: Verify

After recording or uploading, dial *99 to listen to your recording.

If you wish to re-record your message, dial *77

Step 3: Name

Name this Recording:

Click "SAVE" when you are satisfied with your recording Save

4.3.8 Teléfonos y terminales

4.3.8.1 Teléfonos IP

Los teléfonos que utilizaremos para realizar llamadas a través de Asterisk serán los Snom m3.

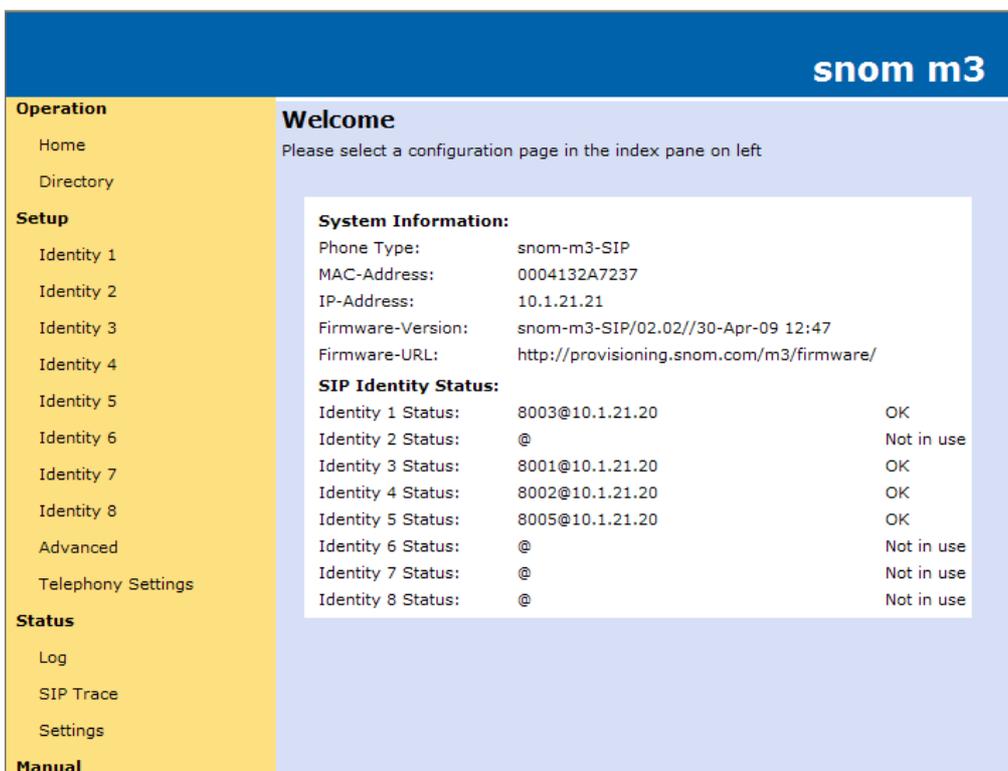
Son teléfonos IP inalámbricos. Una base acepta hasta 8 cuentas SIP ya puede tener 8 teléfonos conectados a las vez y 3 en conversación.



Tienen un alcance de 50 metros en interior y 100 metros en exterior.

Para asignar un teléfono a una extensión configurara en Asterisk tenemos que entrar primero en la página de configuración de la base de los Snom. Para llegar tenemos que poner en un explorador <http://ipasignadaalabase>. Nos pide usuario y contraseña que por defecto es admin/admin.

Al entrar vemos la siguiente pantalla:



The screenshot shows the web interface for a Snom m3 phone. The top right corner has the text "snom m3". On the left is a navigation menu with sections: "Operation" (Home, Directory), "Setup" (Identity 1-8, Advanced, Telephony Settings), "Status" (Log, SIP Trace, Settings), and "Manual". The main content area is titled "Welcome" and contains a "System Information" section and a "SIP Identity Status" section.

System Information:		
Phone Type:	snom-m3-SIP	
MAC-Address:	0004132A7237	
IP-Address:	10.1.21.21	
Firmware-Version:	snom-m3-SIP/02.02//30-Apr-09 12:47	
Firmware-URL:	http://provisioning.snom.com/m3/firmware/	

SIP Identity Status:		
Identity 1 Status:	8003@10.1.21.20	OK
Identity 2 Status:	@	Not in use
Identity 3 Status:	8001@10.1.21.20	OK
Identity 4 Status:	8002@10.1.21.20	OK
Identity 5 Status:	8005@10.1.21.20	OK
Identity 6 Status:	@	Not in use
Identity 7 Status:	@	Not in use
Identity 8 Status:	@	Not in use

En el cuadro blanco que hay en el centro de la imagen vemos las extensiones que hay configuradas en la base y si están conectadas a algún teléfono o no.

Para configurar una nueva extensión tenemos que ir a la izquierda en Setup y clicar en una Identity en la cual no haya ya nada configurado.

Una vez allí tenemos que escribir:

- **Display Name:** el nombre que queramos darle a la extensión (normalmente el mismo que el configurado en Asterisk)
- **Account:** el número de la extensión que hemos configurado en Asterisk.
- **Account Name:** el mismo número que en account.
- **Registrar:** aquí tenemos que poner la IP del servidor Asterisk con el que tiene que conectar la base, en nuestro caso es la 10.1.21.20.
- **Autenticacion Username:** el mismo número que en Account.

Por ejemplo, la página de configuración de la extensión 8003 queda:

The screenshot shows the 'Configuration Identity 1' page in the Asterisk web interface. The form contains the following fields and values:

- Server is local: Yes (dropdown)
- Display Name: Centralita 2 (text input)
- Account: 8003 (text input)
- Password: **** (password input)
- Account Name: 8003 (text input)
- Account Mailbox Name: (empty text input)
- Account Mailbox Number: (empty text input)
- Registrar: 10.1.21.20 (text input)
- Outbound Proxy: (empty text input)
- Authentication Username: 8003 (text input)
- Server Port: 5060 (text input)
- Outbound Proxy Port: 5060 (text input)
- Re-registration time: 600 (text input)
- Registrar Config: Force domain (dropdown)
- DTMF Signalling: RFC 2833 (dropdown)
- Codec Priority: PCMA (text input)
- Buttons: Up, Down, Reset, Remove
- Enable Silence Suppression: No (dropdown)
- Calling Line Identification Restriction: (Section header)
- CLIR: Enable (dropdown)
- CLIR prefix code: (empty text input)
- Call Forwarding: (Section header)
- Forward on busy activate: (empty text input)
- Forward on busy deactivate: (empty text input)
- Forward on no answer activate: (empty text input)
- Forward on no answer deactivate: (empty text input)
- Forward unconditional activate: (empty text input)
- Forward unconditional deactivate: (empty text input)
- Buttons: Save, Cancel, Reboot

Una vez configurada solo tenemos que reiniciar la base.

Para asignar un teléfono inalámbrico a dicha extensión primero tenemos que conectar el teléfono a la base para ello hay que encender el teléfono y se pondrá a buscar una base solo. Reiniciamos la base y el teléfono ya estará conectado a la base y configurado con el número de extensión que hemos configurado recientemente.

4.3.8.2 Softphone



Como softphones para Asterisk utilizaremos los X-Lite. Hemos escogido esta marca ya que es un software gratuito y ampliamente utilizado por los usuarios que necesitan un softphone.

Para descargarlo vamos a la página <http://www.counterpath.com/x-lite-4-for-windows-download.html>.

Una vez descargado e instalado procederemos a configurarlo. Para ello abrimos el softphone y vamos a **Softphone > Accounts Settings**.

Una vez allí la primera pestaña es **Account** aquí tenemos que configurar los datos para que el softphone se pueda conectar a Asterisk. Para ello configuramos:

- **Account Name:** es el número de extensión que le hemos asignado en Asterisk.
- **User ID:** es también el número de extensión que le hemos asignado en Asterisk
- **Domain:** es la IP o el nombre de la máquina Asterisk. En nuestro caso es 10.1.21.20.
- **Display Name:** el nombre que queramos que tenga la extensión cuando llamemos.
- **Authorization Name:** es el password que le hemos asignado en Asterisk cuando hemos configurado la extensión.

Las demás opciones las dejamos por defecto. Una vez configurado para saber si ya ha conectado con Asterisk podemos ver un icono verde que pone Available.

4.3.9 Flash Operator Channel (FOP)

Con el Flash Operator Panel podemos monitorear el comportamiento de FreePBX en ese momento, el estado de los usuarios y poder realizar operaciones sobre las comunicaciones.

La información que podemos ver en FOP es:

- Las extensiones que están llamando, ocupadas o disponibles
- Si una extensión esta ocupada nos indica quien le esta llamando
- Las colas configuradas y su estado
- Los trunks configurados y su estado
- Las conferencias configuradas y su estado
- Los parking lot configurados y su estado

Para acceder al FOP tenemos que ir a la pantalla principal de FreePBX y clickar en Flash Operator Panel (FOP) o también dentro de administración de FreePBX en la pestaña “Panel”.

The screenshot displays the Flash Operator Panel (FOP) interface. At the top right, it indicates "No timeout". The interface is organized into several sections:

- Extensions (Purple background):** Lists five extensions with their status (green for available, red for busy), name, and call duration.

Extension	Status	Name	Duration
8000	Available	Centralita	00:00:18
8001	Busy	Gonzalo Calvo	00:00:03
8002	Available	Phone 2	
8003	Available	Centralita	
8004	Available	Toxico	
8005	Available	Distribucion	00:00:42
- Queues (Pink background):** Shows one queue named "ColaCentralita" with a status icon.
- Conferences (Teal background):** Currently empty.
- Parking lots (Yellow background):** Currently empty.
- Trunks (Green background):** Lists four trunks with their status and call duration.

Trunk	Status	Duration
CallManagerTrunkBcn	Available	
CallManagerTrunkMadrid	Available	
CallManagerBcn	Available	
CallManagerMadrid	Busy	00:00:07

En esta imagen podemos ver que estan ocupadas las extensiones 8000, 8001 y 8005 y esta ocupado el trunks del Call Manager con Madrid y los minutos que llevan hablando cada uno.

4.3.10 Report de llamadas

Para ver los reports tenemos que estar dentro de administración de FreePBX y una vez allí clicar en la pestaña “Report”.

Dentro de Reports diversas pestañas de información:

- **Call logs:** Aquí encontramos el log de todas las llamadas realizadas en un determinado espacio de tiempo. Este log podemos filtrarlo de muchas formas: por un rango de meses, por un rango de días, por el origen (extensión que realiza la llamada), destino (las llamadas recibidas por una extensión), por el canal por el cual se ha hecho las llamadas, o por el rango de duración de las llamadas.

Calldate	Channel	Source	Clid	Dst	Disposition	Duration
2311-11-18 18:11:37	SIPCallMs...	2216	"Sistemas Londres 28" <2216>	8001	ANSWERED	02:12
2311-11-18 18:11:25	SIPCallMs...	2211	"Alberto Martin" <2211>	8001	ANSWERED	00:11
2311-11-18 18:11:14	SIP8002-C...	8032	"Phone 2" <8002>	8000	BUZY	00:00
2311-11-18 18:10:49	SIP8005-C...	8035	"Distribucion" <8005>	8000	ANSWERED	00:46
2311-11-18 18:10:39	SIP8001-C...	8031	"Gonzalo Calvo" <8001>	8000	NO ANSWER	00:03
2311-11-18 18:04:38	SIP8001-C...	8031	"Gonzalo Calvo" <8001>	8000	BUZY	00:00
2311-11-18 18:04:31	SIP8002-C...	8032	"Phone 2" <8002>	8000	ANSWERED	00:12
2311-11-18 15:58:29	SIP8001-C...	8031	"Gonzalo Calvo" <8001>	8000	BUZY	00:00
2311-11-18 15:58:23	SIP8002-C...	8032	"Phone 2" <8002>	8000	ANSWERED	00:11
2311-11-18 15:58:24	SIP8001-C...	8031	"Gonzalo Calvo" <8001>	8000	BUZY	00:00
2311-11-18 15:58:18	SIP8002-C...	8032	"Phone 2" <8002>	8000	ANSWERED	01:59
2311-11-18 15:54:56	SIP8001-C...	8031	"Gonzalo Calvo" <8001>	8000	BUZY	00:00
2311-11-18 15:54:49	SIP8002-C...	8032	"Phone 2" <8002>	8000	ANSWERED	00:14
2311-11-18 15:54:40	SIP8002-C...	8032	"Phone 2" <8002>	8000	BUZY	00:00
2311-11-18 15:53:39	SIP8002-C...	8032	"Phone 2" <8002>	8000	BUZY	00:00
2311-11-18 15:53:31	SIP8001-C...	8031	"Gonzalo Calvo" <8001>	8000	ANSWERED	01:11
2311-11-18 15:46:00	SIP8000-C...	8030	"Centralita" <8000>	*69	ANSWERED	00:06
2311-11-18 15:45:45	SIP8000-C...	8030	"Centralita" <8000>	*77	ANSWERED	00:07
2311-11-18 15:41:33	SIP8000-C...	8030	"Centralita" <8000>	*77	ANSWERED	00:07
2311-11-18 15:41:11	SIP8000-C...	8030	"Centralita" <8000>	*77	ANSWERED	00:07
2311-11-18 15:40:40	SIP8000-C...	8030	"Centralita" <8000>	*77	ANSWERED	00:05
2311-11-18 15:30:01	SIP8000-C...	8030	"Centralita" <8000>	*69	ANSWERED	00:07
2311-11-18 15:29:48	SIP8000-C...	8030	"Centralita" <8000>	*77	ANSWERED	00:07
2311-11-18 15:25:07	SIPCallMs...	2216	"Sistemas Londres 28" <2216>	8001	ANSWERED	03:13
2311-11-18 15:10:10	SIP8002-C...	8032	"Phone 2" <8002>	8000	NO ANSWER	00:02

Si bajamos por la página nos encontramos con el total de minutos de llamadas de cada día del filtro que hayamos escogido, en el caso de nuestra captura es del mes de noviembre de 2011.

TOTAL				
DATE	DURATION	ASTERISK MINUTES		
		GRAPHIC	CALLS	ACT
2011-11-03	02:34		4	00:38
2011-11-07	01:31		15	00:06
2011-11-08	02:05		34	00:03
2011-11-09	29:51		83	00:21
2011-11-10	08:19		6	01:23
2011-11-11	10:17		5	02:03
2011-11-14	81:43		35	02:20
2011-11-15	84:56		16	05:18
2011-11-16	23:59		41	00:35
TOTAL	245:15		239	01:01

[Export PDF file](#)
[Export CSV file](#)

Como podemos observar, nos permite pasar todo los logs del filtro a un pdf o a una hoja CSV.

- **Compare Calls:** Nos permite obtener una gráfica resultante de comparar las llamadas con opción de filtro por destino, origen y canal, de un día y los días anteriores que queremos ver.

Si por ejemplo queremos ver los minutos que ha llamado la extensión 8001 en los últimos 10 días:

Select the day From: 16 November-2011 Laps of days to compare: -10 days

DESTINATION: Exact Begins with Contains Ends with

SOURCE: 8001 Exact Begins with Contains Ends with

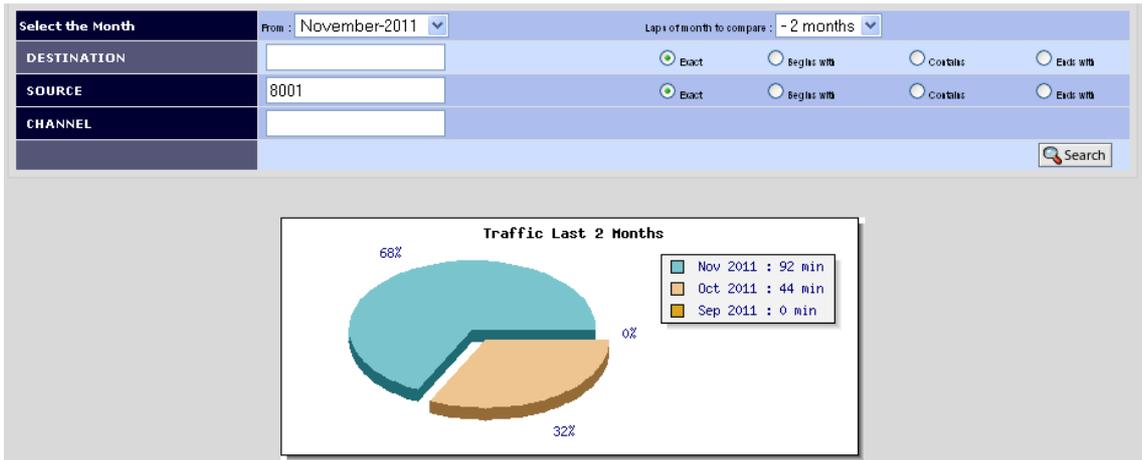
CHANNEL:

Graph: Number of calls by hours

TOTAL				
DATE	DURATION	ASTERISK MINUTES		
		GRAPHIC	CALLS	ACT
2011-11-07	01:01		9	00:06
2011-11-09	06:37		13	00:30
2011-11-10	00:05		2	00:02
2011-11-11	10:06		4	02:31
2011-11-14	09:50		19	00:31
2011-11-15	59:29		3	19:49
2011-11-16	04:51		17	00:17
TOTAL	91:59		67	01:22

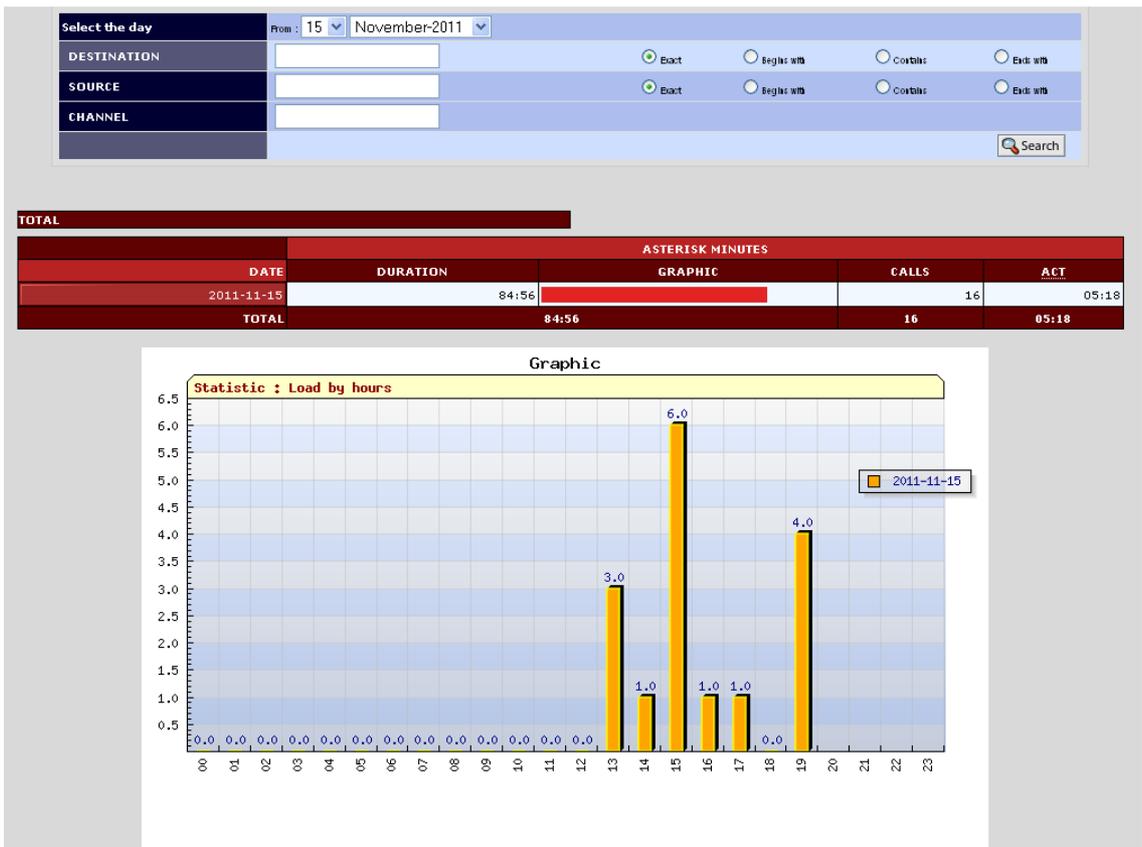
- **Monthly Traffic:** Como su propio nombre indica nos indica el tráfico de llamadas en minutos de un mes y los meses anteriores que elijamos con opción de filtro por destino, origen y canal.

Si por ejemplo queremos ver las llamadas que ha realizado la extensión 8001 en los dos últimos meses:



- **Daily Load:** nos da un gráfico por horas de las llamadas realizadas en un día. De esta forma es fácil ver las horas del día en que hay más actividad telefónica.

En este caso como ejemplo sacaremos el gráfico todas las llamadas de un día.



5 MONITORIZACIÓN CON NAGIOS

Al ser el Call Manager de Cisco y Asterisk las herramientas que utilizaremos para realizar llamadas, son servidores críticos por lo que necesitaremos monitorizarlos para actuar con la mayor brevedad posible ante cualquier inconveniente que aparezca.

Para la monitorización de toda la red de Labco ya tenemos un servidor Nagios, dicho servidor lo utilizaremos para monitorizar ambos sistemas de telefonía.

5.1 ¿Qué es Nagios?

Nagios es una solución GNU GPL (ver Definición 1.3) para la monitorización de equipos y servicios. Entre sus funcionalidades destacamos (extraídas de la documentación del sistema):

- Permite monitorizar los principales servicios de red.
- Permite monitorizar el estado de los recursos del sistema.
- Realiza los chequeos mediante un sistema de plugins ampliable, y que además, permite la realización de tests en paralelo.
- Permite definir una jerarquía entre los hosts, sabiendo distinguir entre servidores caídos e inalcanzables.
- Permite el envío de avisos mediante mail y/u otro sistema definido por el usuario.
- Permite usar “*event handlers*” y la rotación automática de los logs.
- Soporte para usar servidores redundantes para monitorizar y/o realizar monitorización distribuida.
- Permite, de forma opcional, consultar el estado del sistema mediante un interfaz web.

5.2 Instalación y configuración de SNMP en Asterisk

Para poder monitorizar Asterisk y que Nagios nos muestre qué servicios están funcionando correctamente o no. Primero tenemos que activar el servicio SNMP¹⁸ para poder realizar las consultas con Nagios.

Para empezar miramos si tenemos el modulo `res_snmp` instalado y cargado en Asterisk:

```
asterisk -rvvvvvvvvvvvvvvvvv
```

```
CLI> module show like snmp
```

Si aparece:

```
snmp*CLI> module show like snmp
Module                               Description
0 modules loaded
snmp*CLI> quit
Executing last minute cleanups
```

Significa que no lo tenemos. Salimos de la consola:

```
CLI> quit
```

Paramos Asterisk:

```
/etc/init.d/asterisk stop
```

Instalamos los paquetes que se necesitan para la instalación del modulo `res_snmp`:

```
yum install net-snmp net-snmp-devel net-snmp-libs net-snmp-perl net-snmp-utils
```

Entramos en la carpeta de las fuentes de Asterisk y volvemos a compilar:

```
cd /usr/src/asterisk-1.8.7.0
```

```
make distclean
```

```
./configure
```

```
make menuselect
```

En la ventana que aparece nos aseguramos que el modulo `res_snmp` esté activado:

¹⁸ El Protocolo Simple de Administración de Red o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas.

Applications	[*] res_adsi
Call Detail Recording	[*] res_ael_share
Channel Drivers	[*] res_agi
Codec Translators	[*] res_clioriginate
Format Interpreters	[*] res_config_curl
Dialplan Functions	[*] res_config_ldap
PBX Modules	[*] res_config_ldap
Resource Modules	[*] res_config_odbc
Test Modules	[*] res_config_pgsql
Voicemail Build Options	XXX res_config_sqlite
Compiler Flags	[*] res_convert
Module Embedding	[*] res_crypto
Core Sound Packages	[*] res_indications
Music On Hold File Packages	[*] res_jabber
Extras Sound Packages	[*] res_limit
	[*] res_monitor
	[*] res_musiconhold
	[*] res_odbc
	[*] res_phoneprov
	[*] res_realtime
	[*] res_smdi
	[*] res_snmp
	[*] res_speech

Salimos de la ventana y seguimos:

make

make install

Volvemos a arrancar Asterisk y averiguamos si ahora el modulo está cargado:

/etc/init.d/asterisk start

asterisk -rvvvvvvvvvvvvv

CLI> module show like snmp

Esta es la salida:

```
snmp*CLI> module show like snmp
Module                Description
res_snmp.so           SNMP [Sub]Agent for Asterisk
1 modules loaded
```

Salimos de la consola de Asterisk y configuramos el archivo res_snmp.conf

CLI> quit

nano /etc/asterisk/res_snmp.conf

Y descomentamos las siguientes líneas:

```
[general]
subagent = yes
```

```
enabled = yes
```

Guardamos los cambios y creamos los archivos con los OID de Asterisk en la carpeta de snmp. Un OID (identificador de objeto) es una cadena alfanumérica que se utiliza para identificar de forma única un objeto.

En la carpeta

```
/usr/share/snmp/mibs
```

```
vi asterisk-mib.txt
```

Copiar y pegar el código mib de la página:

<https://wiki.asterisk.org/wiki/display/AST/Asterisk+MIB+Definitions>

```
vi digium-mib.txt
```

Copiar y pegar el código mib de la página:

<https://wiki.asterisk.org/wiki/display/AST/Digium+MIB+Definitions>

Ahora configuramos SNMP de modo que pueda interactuar con Asterisk:

```
cd /etc/snmp
```

movemos el archivo de configuración de default:

```
mv snmpd.conf snmpd.conf.old
```

y creamos en nuestro:

```
nano snmpd.conf
```

Poniendo las siguientes líneas:

```
rwcommunity private 127.0.0.1  
rocommunity public  
disk /  
master agentx  
agentXSocket /var/agentx/master  
agentXPerms 0660 0550 root asterisk  
com2sec local localhost public  
com2sec remote 128.0.0.1 public
```

```
group asterisk v1 remote  
group asterisk v2c remote  
group NetWork v1 remote  
group NetWork v2c remote  
view all included .1  
access asterisk "" any noauth exact all none none  
access NetWork "" any noauth exact all none none  
sysObjectID .1.3.6.1.4.1.22736.1
```

Primero definimos el agente y los permisos de acceso. Luego definimos dos comunidades. Una tiene acceso local y otra remoto. Como nuestro servidor Nagios esta de forma remota le ponemos la ip de éste (128.0.0.1).

Guardamos los cambios y arrancamos SNMP:

```
/etc/init.d/snmpd start
```

Volvemos el arranque automático:

```
chkconfig snmpd on
```

Y por ultimo reiniciamos Asterisk:

```
/etc/init.d/asterisk restart
```

Para ver los resultados con la descripción de los OID en lugar de los números de los objetos:

```
export MIBS=all
```

Ahora ya podemos hacer una consulta utilizando el OID de Asterisk para comprobar que funciona correctamente el SNMP:

```
snmpwalk -OT -c public -v 2c localhost .1.3.6.1.4.1.22736
```

5.3 Configuración de Nagios para la monitorización de Asterisk

Para configurar la monitorización, necesitamos los plugins de Nagios que se encuentran en `/usr/local/nagios/libexec`, configurar los comandos, los hosts y los servicios. Éstos últimos se encuentran en `/usr/local/nagios/etc`.

Para conocer la sintaxis de un plugin de nagios siempre debemos hacer:

```
./check_snmp -h
```

5.3.1 Script de comprobación de conexión de los trunks

Este script se utilizará para comprobar que los trunks siguen conectados. Tenemos que ejecutar un comando en Asterisk desde Nagios, por lo que como tenemos que ejecutar un comando en una máquina remota utilizaremos `openssh` para realizar la conexión segura.

Como el comando hay que ejecutarlo como `root` al realizar el comando `ssh` nos pedirá autenticación, pero al ser la monitorización remota no podemos ir poniendo siempre la contraseña para que compruebe el comando, por lo que tenemos que hacer uso de criptografía de clave pública.

El proceso es sencillo, lo único que tenemos que hacer es generar un par de claves públicas para que cuando Nagios intente ejecutar un comando que necesite autenticación al tener ambos el par de claves públicas no pida contraseña y el comando se ejecute sin problemas.

Para generar los pares de claves se empleará el programa `ssh-keygen`. Para crear las claves en Nagios utilizaremos el comando `ssh-keygen -t rsa`.

```
[root@nagios ssh_keys]# ssh-keygen -t rsa  
Generating public/private rsa key pair.  
Enter file in which to save the key (/root/.ssh/id_rsa):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /root/.ssh/id_rsa.
```

Your public key has been saved in /root/.ssh/id_rsa.pub.

The key fingerprint is:

ed:79:c8:de:4c:c5:14:df:f6:82:56:58:ad:90:5c:b6 root@nagios.grupo.general-lab.com

Una vez ejecutado este comando tendremos las claves en **/root/.ssh**.

Para poder acceder al servidor sin contraseña deberemos añadir la clave pública al fichero **/root/.ssh/authorized_keys**, para ello:

```
[root@nagios etc]#scp /root/.ssh/id_rsa.pub root@10.1.21.20:
user@server's password:
*****
id_rsa-1.pub      100% |*****| 217    00:00
```

Y en Asterisk:

```
[root@asterisk ~]#mkdir /root/.ssh
[root@asterisk ~]#cat root/idrsa-1.pub >> root/.ssh/authorized_keys
```

Ahora ya tenemos toda la estructura de llave pública instalada.

Lo siguiente que haremos es crear el archivo **check_trunk_asterisk.sh**.

```
cd /usr/local/nagios/libexec
```

```
vi check_trunk_asterisk.sh
```

Introducimos el siguiente código:

```
#!/bin/bash
# Este es un script para ver si los trunks de Asterisk esta activos.
TRUNK_NAME=$1
STATUS=`ssh root@10.1.21.20 'asterisk -rx "sip show peers"|grep -a
'$TRUNK_NAME'|awk {'print $2}'`

if [ -n $STATUS ]; then
    echo "SIP Trunk OK."
    exit 0
else
    echo "SIP Trunk DOWN."
```

```
    exit 2
fi
```

Este script coge el nombre del trunk que le pasamos por el fichero de services.cfg, como veremos más adelante, e introduce ese nombre en la variable TRUNK_NAME.

Lo siguiente que hace es hacer una consulta ssh al servidor Asterisk y con un grep comprueba que se encuentre el nombre del trunk en la consulta a Asterisk y se queda con la segunda columna que es la dirección IP del trunks.

Más tarde hacemos una consulta condicional en la que si la variable STATUS, que es donde hemos introducido la dirección IP del trunk, no esta vacía, entonces el trunk esta activo y sacamos un exit = 0, para que en la página de Nagios nos aparezca el servicio como OK.

Si la variable STATUS esta vacía querrá decir que ese trunk no esta activo, ya que al hacer la consulta ssh si el trunk no esta activo dicho trunk no aparece, por lo que sacamos el texto de que el trunk esta caído y sacamos un exit = 2 para que en la página de Nagios aparezca el servicio inactivo y nos mande un aviso.

Ahora tenemos que asignar el script a un comando en el archive checkcommands.cfg.

```
vi /usr/local/nagios/etc/checkcommands.cfg
```

Y en el archivo añadimos:

```
#'check_turnk_asterisk' command definition
define command{
command_name check_trunk
command_line $USER1$/check_trunk_asterisk.sh $ARG1$
}
```

Con el argumento \$ARG1\$ cogeremos el primer parámetro que le indiquemos al script a través del archivo de services.cfg.

El siguiente paso consiste en añadir los servicios de monitorización de los dos trunks que tenemos configurados para ello:

```
vi /usr/local/nagios/etc/services.cfg
```

Una vez allí añadimos los siguientes servicios:

```
define service{
```

```
use                generic-service
host_name          AsteriskPBX
service_description Barcelona_Trunk_Check
is_volatile        0
check_period       24x7
max_check_attempts 3
normal_check_interval 5
retry_check_interval 1
contact_groups     admin-nagios
notification_interval 120
notification_period 24x7
notification_options w,c,r
check_command      check_trunk!CallManagerBcn
}
```

define service{

```
use                generic-service
host_name          AsteriskPBX
service_description Madrid_Trunk_Check
is_volatile        0
check_period       24x7
max_check_attempts 3
normal_check_interval 5
retry_check_interval 1
contact_groups     admin-nagios
notification_interval 120
notification_period 24x7
notification_options w,c,r
check_command      check_trunk!CallManagerMadrid
}
```

5.3.2 Script de comprobación de conexión de Asterisk

Este primer script comprobará que Asterisk no está apagado o sin conexión.

Para ello, primero crearemos el plugin `check_asterisk.pl`. Para ello vamos a la página: <http://www.koders.com/perl/fid6B007CE5057236BD89D0945DBDF9951FCC8FDF12.aspx>

```
cd /usr/local/nagios/libexec
```

```
vi check_asterisk.pl
```

Y pegamos el código que encontramos en esta página. Éste plugin también lo podemos conseguir haciendo `yum install nagios-plugins`. Este comando nos bajará todos los plugins que tiene Nagios y entre ellos esta el que nos interesa.

Para añadir los comandos en nagios modificaremos el archivo `checkcommands.cfg`.

```
vi /usr/local/nagios/etc/checkcommands.cfg
```

Y al final del archivo añadimos:

```
define command{
    command_name    check_asterisk
    command_line    $USER1$/contrib/check_asterisk.pl -h $HOSTADDRESS$ -m
                   mgr -u admin -p amp111
}
```

Las opciones de este plugin son:

Command name: nombre del comando

Command line: los parámetros que pasaremos al comando:

- La macro (variable) `$USER1$` contiene el valor `/usr/local/nagios/libexec` especificado en el archivo `/usr/local/nagios/etc/resource.cfg`
- `check_snmp` – Nombre del plugin
- `-H $HOSTADDRESS$` – la opción `-H` define el servidor que vamos a interrogar y `$HOSTADDRESS$` es una macro (variable) predefinida que contiene el nombre del servidor como lo definiremos luego en `localhost.cfg`

- -C public – es la comunidad que vamos a utilizar para conectarnos al agente definido en el archivo /etc/snmp/snmp.conf.
- -o – la OID que vamos a consultar
- -P 2c – versión de SNMP utilizada para la consulta
- -l la etiqueta que definiremos
- -w – está por Warning
- -c – está por Critical
- \$ARG1\$ \$ARG2\$ \$ARG3\$ ARG4\$ son las macros (variables) cuyo valor será asignado desde la configuración de localhost.cfg

Al verificarse el evento Warning y/o Critical, Nagios nos enviará una notificación por correo electrónico.

admin y amp111 indican respectivamente el usuario y la contraseña para conectarse al AMI de Asterisk. Para definirlos tenemos que modificar el manager.conf de Asterisk de la siguiente forma:

vi /etc/asterisk/manager.conf

```
[general]
displayssystemname = yes
enabled = yes
webenabled = yes
port = 5038

[admin]
secret = sesamo
deny=0.0.0.0/0.0.0.0
permit=127.0.0.1/255.255.255.255
read = system,call,log,verbose,command,agent,user,config
write = system,call,log,verbose,command,agent,user,config
```

Ahora tenemos que actualizar la configuración:

amportal restart

Lo siguiente es modificar el archivo hosts.cfg.

```
vi /usr/local/nagios/etc/hosts.cfg
```

Y añadimos las siguientes líneas:

```
define host{
    use          generic-host
    host_name    AsteriskPBX
    alias       AsteriskPBX_centralita
    address     10.1.21.20
    contact_groups    admin-nagios,guardias
    check_command    check-host-alive
    max_check_attempts    3
    notification_interval    120
    notification_period    24x7
    notification_options    d,r
}
```

Con el check-host-alive sabemos si el servidor está caído o no ya que este comando hace un ping continuo para saber si el servidor esta apagado. En la sección address ponemos la dirección IP de nuestro servidor y con host_name el nombre que le asignamos para poder utilizarlo posteriormente.

Por último, modificaremos el archivo services.cfg.

```
vi /usr/local/nagios/etc/hosts.cfg
```

Y añadimos al final las siguientes líneas:

```
define service{
    use          generic-service
    host_name    AsteriskPBX
    service_description    Asterisk_check
    is_volatile    0
    check_period    24x7
    max_check_attempts    3
    normal_check_interval    5
    retry_check_interval    1
}
```

```

contact_groups      admin-nagios
notification_interval 120
notification_period 24x7
notification_options w,c,r
check_command       check_asterisk
}

```

A través del plugin `check_asterisk` controlamos que el servicio de Asterisk este arrancado y funcionando.

Ahora antes de nada tenemos que comprobar que los archivos de configuración de Nagios que hemos modificados están correctos para ello utilizamos el comando:

```
../bin/nagios -v nagios.cfg
```

Si obtenemos 0 errores como respuesta significa que todo esta bien y ya podemos reiniciar el servicio de nagios. En caso contrario nos indica el archivo y la línea del error.

Ahora solo nos falta reiniciar primero Apache y después Nagios:

```
/etc/init.d/httpd restart
```

```
/etc/init.d/nagios restart
```

Abrimos un navegador e introducimos <http://nagios/nagios/> y comprobamos que los servicios que teníamos que monitorizar se están monitorizando correctamente.

En la próxima imagen vemos que todos los servicios están monitorizados y funcionando.

The screenshot shows the Nagios web interface with the following sections:

- Current Network Status:** Last Updated: Wed Oct 2 17:10:58 CEST 2013. Updated every 60 seconds. Nagios® - www.nagios.org. Logged in as informatica.
- Host Status Totals:**

Up	Down	Unreachable	Pending
1	0	0	0
All Problems		All Types	
0		1	
- Service Status Totals:**

Ok	Warning	Unknown	Critical	Pending
4	0	0	0	0
All Problems		All Types		
0		4		
- Service Status Details For Host 'AsteriskPBX':**

Host ↑ ↓	Service ↑ ↓	Status ↑ ↓	Last Check ↑ ↓	Duration ↑ ↓	Attempt ↑ ↓	Status Information
AsteriskPBX	Asterisk_check	OK	02-10-2013 17:08:53	2d 3h 0m 43s	1/3	OK (idle)
	Barcelona_Trunk_Check	OK	02-10-2013 17:07:44	0d 0h 3m 14s	1/3	SIP Trunk OK.
	Madrid_Trunk_Check	OK	02-10-2013 17:09:19	0d 0h 1m 39s	1/3	SIP Trunk OK.
	PING	OK	02-10-2013 17:10:39	0d 17h 23m 26s	1/3	PING OK - Packet loss = 0%, RTA = 10.02 ms

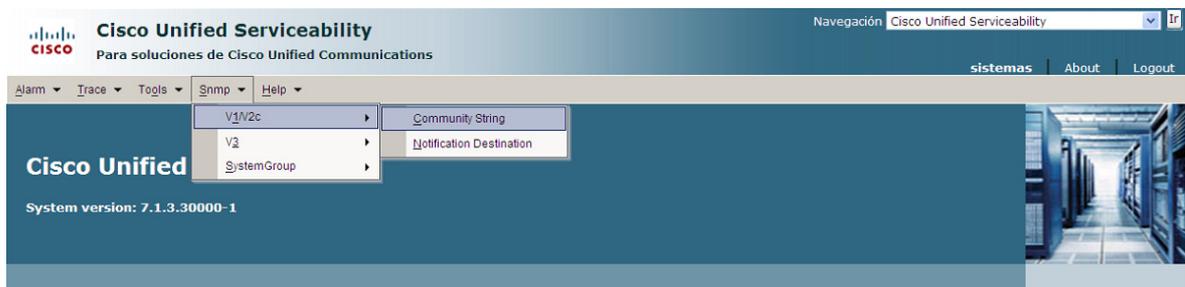
5.4 Configuración SNMP en Cisco Call Manager

Necesitaremos monitorizar las centralitas Cisco con el Nagios también. Para ello primero necesitaremos activar el SNMP en las centralitas de Barcelona y de Madrid.

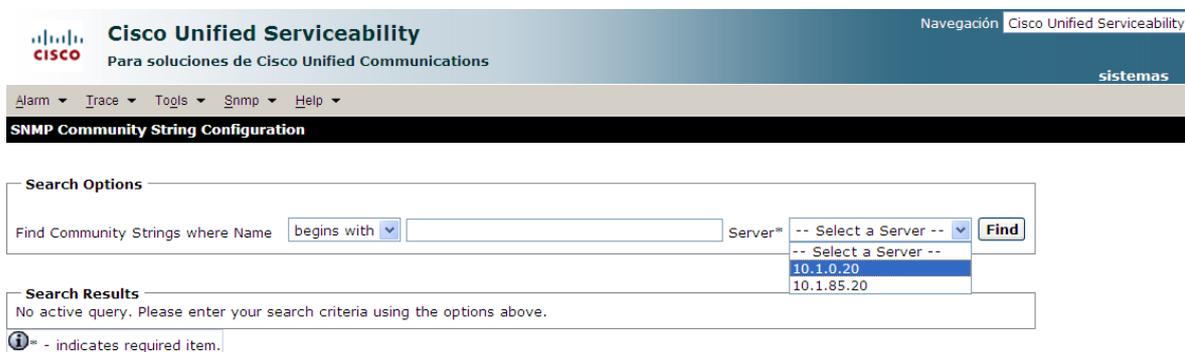
Vamos a la pantalla de configuración del Call Manager y elegimos la opción “Cisco Unified Serviceability”

Una vez allí vamos a:

Snmp > V1/V2c > Community String



Una vez allí seleccionamos el servidor que queremos configurar y pulsamos “find”



Apretamos al botón de añadir y una vez ahí configuramos nuestra “Community String”, la de Barcelona quedará de la siguiente forma:

Cisco Unified Serviceability
Para soluciones de Cisco Unified Communications

Alarm Trace Togs Snmp Help

SNMP Community String Configuration

Save Clear All Cancel

Status
Status : Ready

Server* 10.1.0.20

Community String Information
Community String CiscoCallManagerBarcelona

Host IP Addresses Information
 Accept SNMP Packets from any host
 Accept SNMP Packets only from these hosts
 Host IP Address
 Insert
 Host IP Addresses
 128.0.0.1
 Remove

Access Privileges
 Access Privileges* ReadOnly
 Notify access privilege is required in order to configure Notification Destinations.

Apply To All Nodes

Save Clear All Cancel

* - indicates required item.

Como podemos ver al Community String le añadimos la ip de nuestro Nagios para que acepte los paquetes SNMP y le pondremos privilegios solo de lectura, ya que no necesitamos hacer nada más que leer las notificaciones SNMP.

5.5 Configuración en Nagios para la monitorización de Cisco Call Manager

Igual que al configurar Asterisk primero tenemos que crear los dos host de los Cisco Call Manager de Madrid y Barcelona.

Para ello en Nagios vamos a la ruta **vi /usr/local/nagios/etc/hosts.cfg**. Una vez allí al final del archivo añadimos:

```
define host{
    use                generic-host
    host_name          CCMBarcelona
    alias              CiscoCallManagerbarcelona
    address            10.1.0.20
    contact_groups     admin-nagios,guardias
    check_command      check-host-alive
    max_check_attempts 3
    notification_interval 120
    notification_period 24x7
    notification_options d,r
}
define host{
    use                generic-host
    host_name          CCMMadrid
    alias              CiscoCallManagerMadrid
    address            10.1.85.20
    contact_groups     admin-nagios,guardias
    check_command      check-host-alive
    max_check_attempts 3
    notification_interval 120
    notification_period 24x7
    notification_options d,r
}
```

Ahora solo falta definir los servicios. Monitorizaremos el número de teléfonos registrados, una descripción del sistema, los teléfonos rechazados, los teléfonos no registrados.

vi /usr/local/nagios/etc/checkcommands.cfg

```
define service{
    use                generic-service
    host_name          CCMBarcelona
    service_description Registered Phones
    is_volatile        0
    check_period       24x7
    max_check_attempts 3
    normal_check_interval 5
    retry_check_interval 1
    contact_groups     admin-nagios
    notification_interval 120
    notification_period 24x7
    notification_options w,c,r
    check_command
check_snmp!.1.3.6.1.4.1.9.9.156.1.5.5.0!CiscoCallManagerBarcelona
}

define service{
    use                generic-service
    host_name          CCMBarcelona
    service_description System description
    is_volatile        0
    check_period       24x7
    max_check_attempts 3
    normal_check_interval 5
    retry_check_interval 1
    contact_groups     admin-nagios
    notification_interval 120
    notification_period 24x7
```

```

notification_options      w,c,r
check_command
check_snmp!.1.3.6.1.2.1.1.0!CiscoCallManagerBarcelona
}

define service{
    use                    generic-service
    host_name              CCMBarcelona
    service_description    Rejected Phones
    is_volatile            0
    check_period           24x7
    max_check_attempts     3
    normal_check_interval  5
    retry_check_interval   1
    contact_groups         admin-nagios
    notification_interval  120
    notification_period    24x7
    notification_options   w,c,r
    check_command
check_snmp!.1.3.6.1.4.1.9.9.156.1.5.7.0!CiscoCallManagerBarcelona
}

define service{
    use                    generic-service
    host_name              CCMBarcelona
    service_description    UnRegistered
    is_volatile            0
    check_period           24x7
    max_check_attempts     3
    normal_check_interval  5
    retry_check_interval   1
    contact_groups         admin-nagios
    notification_interval  120
    notification_period    24x7

```

```

notification_options      w,c,r
check_command
check_snmp!.1.3.6.1.4.1.9.9.156.1.5.6.0!CiscoCallManagerBarcelona
}
define service{
    use                    generic-service
    host_name              CCMBarcelona
    service_description    Cisco-VoIP-callmangers
    is_volatile            0
    check_period           24x7
    max_check_attempts     3
    normal_check_interval  5
    retry_check_interval   1
    contact_groups         admin-nagios
    notification_interval  120
    notification_period    24x7
    notification_options   w,c,r
    check_command
check_snmp!.1.3.6.1.4.1.9.9.156.1.1.2.1.4.1!CiscoCallManagerBarcelona
}

```

Los servicios definidos los monitorizamos directamente mediante consultas SNMP. Así podemos ver que monitorizamos el estado del Call Manager, para ver si esta funcionando, también monitorizamos el número de teléfonos registrados, el número de teléfonos rechazados. Estos son los teléfonos que no están bien configurados y que no están funcionando debidamente.

Además también tenemos una descripción del sistema con sus propiedades hardware y el número de teléfonos no registrados.

Para el Call Manager de Madrid hay que poner las mismas líneas pero cambiando CCMBarcelona por CCMMadrid.

La consulta de Nagios queda:



General

- Home
- Documentation

Monitoring

- Tactical Overview
- Service Detail
- Host Detail
- Hostgroup Overview
- Hostgroup Summary
- Hostgroup Grid
- Servicegroup Overview
- Servicegroup Summary
- Servicegroup Grid
- Status Map
- 3-D Status Map
- Service Problems
- Host Problems
- Network Outages

Show Host:
CCMBar

Current Network Status
 Last Updated: Thu Jan 12 18:49:53 CET 2012
 Updated every 60 seconds
 Nagios® - www.nagios.org
 Logged in as *informatica*

[View History For This Host](#)
[View Notifications For This Host](#)
[View Service Status Detail For All Hosts](#)

Host Status Totals

Up	Down	Unreachable	Pending
1	0	0	0
All Problems		All Types	
0		1	

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
5	0	0	0	0
All Problems		All Types		
0		5		

Service Status Details For Host 'CCMBarcelona'

Host ↑↓	Service ↑↓	Status ↑	Last Check ↑↓	Duration ↑	Attempt ↑	Status Information
CCMBarcelona	Cisco-VoIP-callmanagers	OK	12-01-2012 18:42:57	9d 7h 21m 39s	1/3	SNMP OK - "7.1.3.30000-1"
	Registered Phones	OK	12-01-2012 18:48:00	9d 7h 25m 17s	1/3	SNMP OK - 66
	Rejected Phones	OK	12-01-2012 18:47:59	9d 7h 21m 39s	1/3	SNMP OK - 0
	System description	OK	12-01-2012 18:42:58	9d 7h 21m 39s	1/3	SNMP OK - Hardware:762514, 1 Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz, 2048 MB Memory; Software:UCOS 4.0.0.0-28
	UnRegistered	OK	12-01-2012 18:46:42	9d 7h 21m 39s	1/3	SNMP OK - 108

5 Matching Service Entries Displayed

6 ANÁLISIS ECONÓMICO

El impacto económico del proyecto era la pieza clave del proyecto para decidir integrar Asterisk con Cisco.

El análisis económico será una comparación entre ambas plataformas de precios de coste de instalación en una sede con 4 teléfonos, ya que la centralita Asterisk se quiere utilizar para centros de unos 4 o menos teléfonos.

Los apartados que compararemos serán:

- Los servidores de configuración y señalización telefónica
- Los teléfonos IP utilizados para llamadas
- La electrónica de red

6.1 Análisis económico de servidores

El servidor de configuración de las extensiones y de señalización de llamadas que se utiliza para la telefonía IP de Cisco es el Call Manager y el servidor utilizado para las mismas funciones es Asterisk es un servidor HP ProLiant DL140 G3 con la instalación de un Linux y de Asterisk.

6.2 Análisis económico de los teléfonos IP

Los teléfonos IP utilizados en las instalaciones Cisco son los Cisco IP Phone 7911. En cambio, para la telefonía IP con Asterisk se utilizan los Snom M3.

6.3 Análisis económico de la electrónica de red

Para conectar los teléfonos de Cisco con el Call Manager se utilizarán los gateways de dicha marca.

En cambio, para conectar los teléfonos a Asterisk se utilizaran Cisco 5505 para crear una VPN hasta dicho servidor.

6.4 Resumen comparativo de la inversión realizada para un centro

6.4.1 Inversión con Cisco

Dispositivo	Modelo	Unidades	Precio Unidad	Total
Servidor	Cisco CallManager v.7.0	1	3.458,00 €	3.458,00 €
Teléfonos IP	Cisco IP Phone 7911	4	199,95 €	799,80 €
Gateway	Gateway Cisco 1861 Integrated Services Router	1	2.343,17 €	2.343,17 €
			Total	6.600,97 €

6.4.2 Inversión con Asterisk

Dispositivo	Modelo	Unidades	Precio Unidad	Total
Servidor	HP ProLiant DL140 G3	1	954,58 €	954,58 €
Base + Teléfono	Snom M3	1	139,95 €	139,95 €
Teléfonos IP	Snom M3 inalámbricos	3	79,95 €	239,85 €
ASA	Cisco ASA 5505 Firewall Edition	1	295,00 €	295,00 €
			Total	1.629,38 €

6.4.3 Resultados

En total implementar un centro con las características que se ha enumerado anteriormente con Cisco, cuesta unos 6.600 € y instalar el mismo centro con tecnología Asterisk cuesta unos 1.629 €.

Vemos claramente que es mucho más barato implementar el sistema Asterisk en nuestros centros, del orden de cinco veces más barato que poner Cisco.

Por lo tanto, al comenzar el proyecto las previsiones de que instalar Asterisk en este tipo de centros si que salía a cuenta se han cumplido.

7 CONCLUSIONES Y FUTURO

7.1 Conclusiones

A fecha de hoy, desde que se decidió llevar a cabo el proyecto de migrar toda la telefonía de la empresa a VoIP, se han logrado alcanzar todos los objetivos marcados excepto uno.

- Se han cambiado las comunicaciones de la empresa a una tecnología más novedosa y rápida
- Gracias al cambio en la rapidez y calidad de servicio de las comunicaciones, se ha podido cambiar toda la telefonía de la empresa, pasando de una telefonía analógica en la que se pagaba por las llamadas realizadas, a una telefonía digital en la que solo se paga por la conexión de datos.
- Para los centros en los que se necesitan conectar tres o cuatro teléfonos, se ha implementado una centralita Asterisk y se ha integrado dentro de la estructura ya implementada de Cisco para poder realizar llamadas entre las dos infraestructuras.
- La implementación de Asterisk al ser con licencia GPL reduce el coste de la telefonía IP respecto a Cisco, en el que se tiene que pagar por cada extensión conectada una licencia.
- La centralita Asterisk no solo esta configurada para transmitir y poder realizar llamadas, sino que también se ha configurado otros servicios de valor añadido como pueden ser música en espera, operadoras virtuales, colas de llamadas, etc.
- La funcionalidad que no se ha podido implementar ha sido la de poder realizar llamadas SIP a través de los teléfonos utilizando la conexión de datos de telefonía móvil 3G.

En un primer momento, se hizo un estudio de cómo poder conectar el teléfono mediante conexión 3G a Asterisk, pero una vez instalado el programa SIP para realizar la conexión salía siempre dentro del programa sin conexión. Al ver este comportamiento del programa decidimos llamar a Movistar, el proveedor de

servicios telefónicos móviles de la empresa y nos comunicaron que Movistar al ver un paquete con formato SIP no dejaba realizar la conexión, por lo que ha sido imposible poder realizar esta funcionalidad.

7.2 Futuro

Una de las políticas de la empresa es tener siempre todos los sistemas por duplicado, para que en caso de fallo del sistema principal, tener otro preparado para no perder el servicio o perderlo el menor tiempo posible. Así pues, en un futuro se tendrá que implementar otro sistema Asterisk que esta conectado en cluster con el sistema implementado en este proyecto.

Con esto se conseguirá que si cae la conexión o el servidor se estropea, el otro servidor automáticamente realice y gestione las llamadas de la compañía.

8 BIBLIOGRAFÍA

- [1] **Asterisk: The Future of Telephony,**
Jim Van Meggelen, Leif Madsen, and Jared Smith, 2007, O'Reilly
- [2] **The Asterisk Handbook, Version 2,**
Mark Spencer, Mack Allison, Christopher Rhodes, 2003, Digium
<http://www.digium.com>
- [3] **Cisco Unified Communications Manager Administration Guide,**
2009 Cisco Systems, Inc.
- [4] **Building Telephony Systems with Asterisk,**
David Gomillion, Barrie Dempster, September 2005, Packt Publishing
- [5] **Cisco Unified Communications Solution Reference Network Design (SRND),** 2009 Cisco Systems, Inc.
- [6] **Como construir y configurar un PBX con software libre Asterisk ver.1.4,**
Flavio E. Gonçalves, 1ª Edición, Enero 2007
- [7] **FreePBX 2.5 Powerful Telephony Solutions,**
Alex Robar, 2009, Packt Publishing
- [8] **Descarga de Asterisk:** <http://www.asterisk.org/>
- [9] **Descarga de CentOS:** <http://www.centos.org/>
- [10] **Documentación Nagios:** <http://www.nagios.org/>
- [11] **Voip-Info.org**
<http://www.voip-info.org/wiki/view/Asterisk+Cisco+CallManager+Integration>
<http://www.voip-info.org/wiki/view/Asterisk+monitoring>
<http://www.voip-info.org/wiki/view/Asterisk+SNMP>
<http://www.voip-info.org/wiki/view/Asterisk+config+sip.conf>
<http://www.voip-info.org/wiki/view/Asterisk+config+extensions.conf>

<http://www.voip-info.org/wiki/view/SCCP-HOWTO2>

[12] Instalación de Asterisk en CentOS

<http://www.selbytech.com/2011/05/how-to-setup-asterisk-1-8-on-centos-5/>

<http://javdroid.wordpress.com/2011/01/27/instalacion-de-centos-5-asterisk-1-8-2-2/>

<http://www.markinthedark.nl/news/ubuntu-linux-unix/69-installing-freepbx-28-with-asterisk-18-on-centos-55.html>

[13] Configuración de Trunks

<http://www.freepbx.org/news/2009-06-07/cisco-unified-cm-6-1-to-asterisk-and-freepbx-sip-trunks-powered-by-bandwidth-com>

<http://www.voicetrunking.com/sip-trunk/freepbx/>

<http://www.freepbx.org/forum/freepbx/users/how-to-connect-my-freepbx-box-with-cisco-voip-gateway>

<http://www.stephenwagner.com/?p=14>

http://www.isaiasrivera.com/index.php?option=com_content&view=article&id=54:troncal-sip-entre-asterisk-y-cisco-voice-gateway&catid=39:cisco-voip&Itemid=57

[14] Conexiones SNMP para Nagios

<http://voxilla.com/2009/02/03/configuring-asterisk-snmp-support-1131>

<http://forum.pikatechnologies.com/showthread.php?464-Monitoring-FreePBX-with-Nagios>

<http://voztovoice.org/?q=node/296>

<http://voztovoice.org/?q=node/300>

http://www.uv.es/sto/articulos/BEI-2003-01/ssh_np.html