PROYECTO TECNICO

INTEGRACION DE RED TELEMATICA PARA EL CLIENTE “CLIENTE S.A.”

ÍNDICE

1. PROYECTO TÉCNICO

1.1.- Introducción

El presente documento pretende recoger las especificaciones básicas así como la planificación para llevar a cabo el proyecto de integración de una red telemática de comunicaciones, tanto a nivel de voz como de datos, para el cliente CLIENTE S.A.

1.2.- Objetivos

El objetivo del presente proyecto se basa en la prestación de un servicio de comunicaciones integral demandado por el cliente CLIENTE S.A.
Para la implantación de dicho proyecto y la consecución de todos los objetivos, el cliente nos solicita las siguientes funcionalidades dentro de su red de comunicaciones.

- Red corporativa VPN-IP con accesos Fibra y ADSL.

La distinción del tipo de acceso a la red se hará en función del número de usuarios presentes en cada delegación de cliente, así como de la importancia de dicha oficina en el negocio de cliente. En un primer momento se ha pensado dotar de accesos de Fibra con mayores velocidades a los puntos centrales, siendo esta velocidad de acceso de 20 Mb. Para el resto de oficinas se ha pensado, a raíz de los requerimientos de cliente, en un acceso ADSL con velocidades de 10 Mb en bajada y 1 Mb en subida. Estos accesos pueden llegar a variar en función de la cobertura disponible en cada localización de cliente.

Los accesos principales estarán funcionando sobre equipos Cisco2911 y para las sedes remotas se ha pensado en Cisco1921. Para el nodo central se ha pensado en equipos Cisco 3560.

Dentro de las soluciones de backup, las oficinas centrales o tipo 1 tendrían un acceso Fibra con backup ADSL y las oficinas tipo 2 también llamadas oficinas singulares tendrán un acceso ADSL con respaldo RDSI de 256kb.

Además el cliente necesita renovar su infraestructura interna para adaptarla a los requisitos necesarios para una red de telefonía ip, por lo que también es objeto de este proyecto la implantación de una red de switches en todas las oficinas que conecten la red WAN del proveedor con la red LAN de cliente. Se ha pensado en dotar a las oficinas a nivel LAN con equipamiento Cisco de la serie 2960 con POE.

- Acceso a Internet centralizado a través de un caudal compartido en toda la VPN de cliente.

El cliente nos solicita un acceso centralizado a Internet, ya que tiene aplicaciones que deben ser accesibles desde Internet para trato con otros cliente y /o proveedores en su línea de negocio. Además el cliente nos solicita un caudal centralizado de acceso a Internet disponible para la navegación de sus usuarios. Se ha pensado en un primer momento en instalar estos accesos a través de fibra, con un caudal simétrico, tanto ascendente como descendente, de 8 Mb. Este caudal estará redundando a través del acceso de backup de fibra de la oficina central.

- Red de telefonía IP

Para el cliente CLIENTE S.A. es necesario disponer de una red de telefonía IP que les permita realizar llamadas entre las distintas oficinas de su red a coste 0. Para ello es necesario un despliegue tanto de terminales de telefonía, como de centralitas. Dentro de este punto, se propone al cliente una solución basada en Cisco Call Manager, versión 8 con teléfonos ip Cisco desde la gama 7970 hasta la SPA 252G siendo el cliente responsable del reparto de dichos teléfonos dentro de sus usuarios en función de la categoría de éstos.

Para la interconexión entre la red telefónica del cliente y la red telefónica básica, se ha pensado en un enlace NGN que conecte ambas redes. Como backup ante un posible fallo en la red NGN se propondrá al cliente la utilización de telefonía RDSI de supervivencia a través de tarjetas SRST.

1.3.- Esquema red corporativa

Se adjunta documento con el esquema de red propuesto para satisfacer las necesidades del cliente CLIENTE S.A.

Esquema de red.ppt

1.4.- Características de la red - Datos

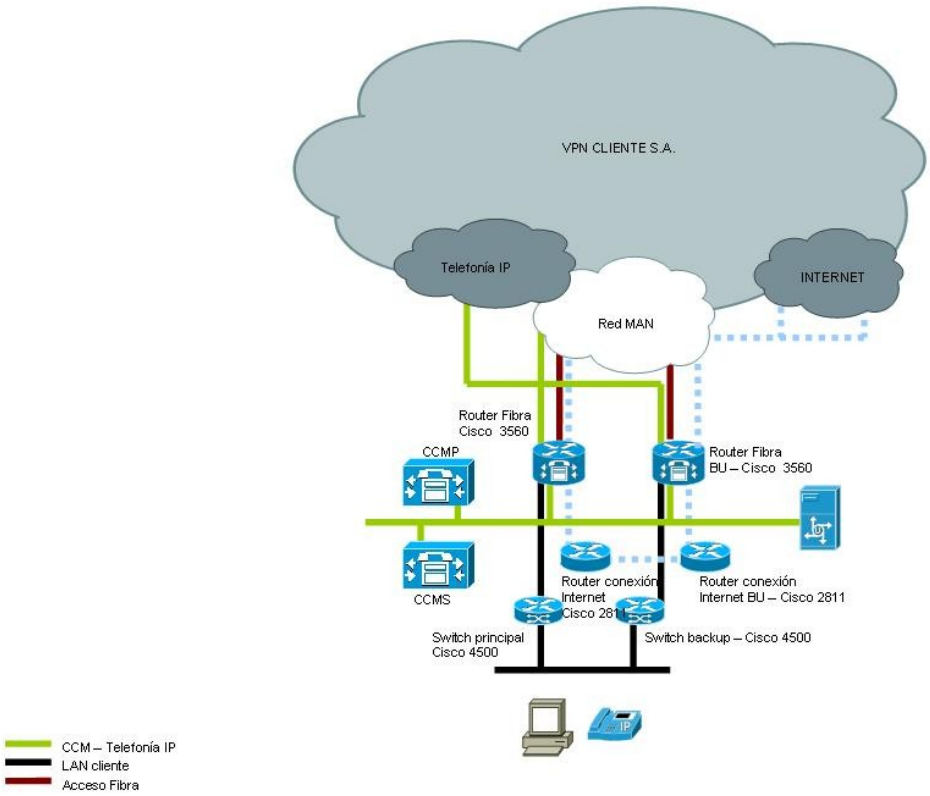
En este apartado se recogen las características básicas de las todas y cada una de las sedes del cliente CLIENTE S.A. Dicha clasificación está realizada en base a los requerimientos del negocio del cliente.

A. SEDE CENTRAL

La sede central del cliente constará de un doble acceso por fibra diversificado. Dicho acceso tendrá un caudal de 80 mb, cuyas calidades se estudiaran en un próximo apartado. Dadas las características de la sede, y al tratarse del nodo central, es preciso que el ancho de banda de la conexión de backup disponga también de 80 mb. Estas conexiones estarán presentes en dos equipos, Cisco 3845.

Además en esta sede irán presentes los 2 equipos de acceso centralizado a internet, ambos sobre un acceso de fibra, con un caudal simétrico de 20 mb. Éste caudal deberá encargarse de soportar la salida a internet tanto de los usuarios de la oficina central como del resto de usuarios de la VPN del cliente. Para este acceso a internet se ha pensado en equipamiento Cisco de la serie 2911 redundado a nivel de fibra y a nivel de equipo.

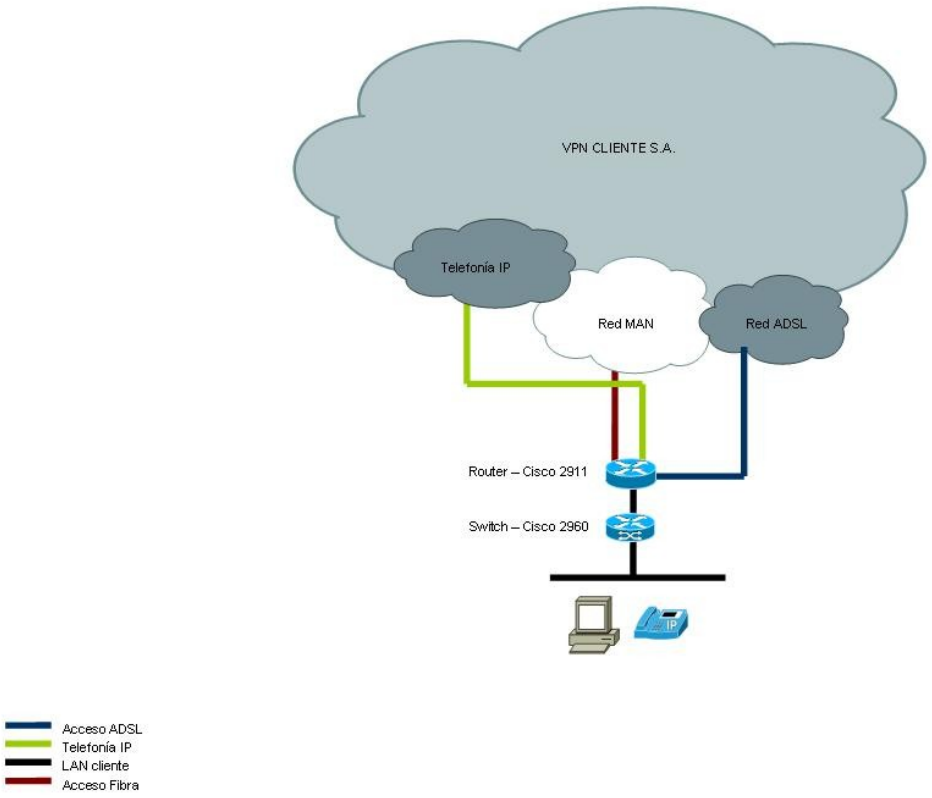
Para la conexión a la parte LAN de cliente, los equipos serán Cisco 4500.
Se ha estimado, para la definición de los caudales, que el volumen de usuarios será de un máximo de 150 dándose como usuarios concurrentes un máximo de 80. Con estos datos, se ha estimado que el trafico sostenido durante una jornada laboral puede estar en torno a los 50 mb, ya que en esta sede van a estar físicamente los servidores (correo, antivirus, bbdd) a los que deben acceder desde el resto de oficinas de la vpn.



B. SEDE TIPO 1

Las sedes tipo 1, contarán con un acceso principal por fibra con un caudal de 20 mb y un backup a través de una línea ADSL con 1Mb en subida y 10 en bajada. Ambas conexiones estarán presentes en un único equipo, de la serie Cisco 2911. A nivel LAN la conexión se hará a través de un Cisco 2960.

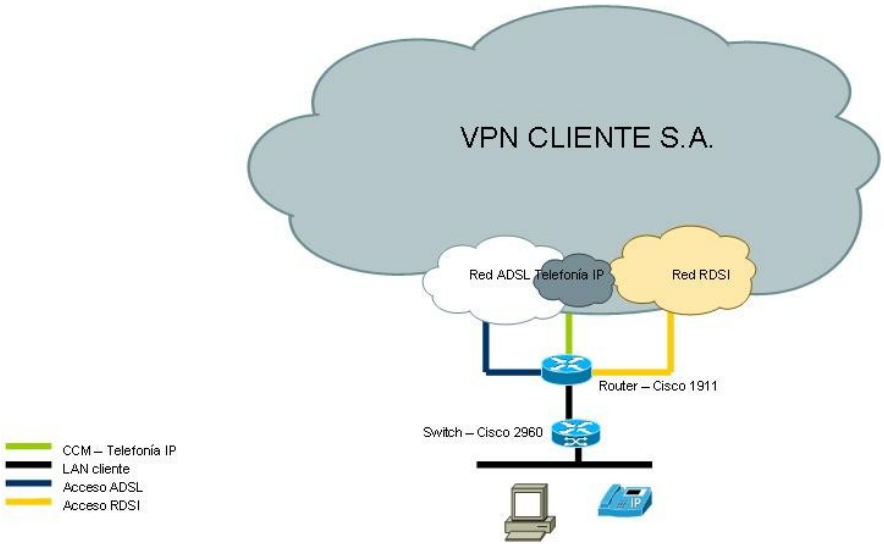
El volumen de usuarios estimado en este tipo de oficinas es de 20 usuarios, de los cuales se ha calculado que puede haber un máximo de 10 usuarios a pleno rendimiento de manera simultánea.



C. SEDE TIPO 2

En este tipo de sede, para el acceso primario se ha pensado en una solución de ADSL (10/1Mb) con respaldo RDSI en el propio equipo. En estas sedes el equipamiento será Cisco de la serie 2811. Al igual que en las sedes tipo 1, la conexión a la LAN se realizará a través de equipos Cisco 2960.

Respecto al volumen de usuarios, se estima que estas sedes podrán tener un máximo de 8 usuarios, de los cuales 4 pueden estar trabajando de manera simultánea.



Nota: Se ha estimado que cada puesto de trabajo, independientemente de la sede a la que pertenezca contará, al menos, con un PC y un terminal de telefonía IP. El resto de posibles terminales, como impresoras o faxes, serán recursos compartidos por un número de usuarios a decidir según las necesidades del negocio de cliente.

1.5.- Características de la red - Voz

Las comunicaciones, a nivel de voz, pasan por la instalación de unas centralitas Cisco Call Manager, versión 8.1 en las dependencias centrales del cliente. Este equipamiento estará redundado, puesto que se ha presupuestado la instalación de un CCM Publisher para el registro de los teléfonos y un CCM Suscriber que almacene y replique la BBDD de la telefonía.

Además de estos equipos, se ha presupuestado la instalación de un Cisco Unity que hará las veces de servidor de mensajería.

- Unified CM 8.5 7845-I3 Appliance – Servidor Publisher
- Unified CM 8.5 7845-I3 Appliance – Servidor Suscriber
- Cisco UCS – B200M2 – Unity

Para la salida de llamadas se ha pensado en dotar a todas las oficinas de acceso a NGN. A continuación se ofrece una breve introducción del servicio NGN así como de los elementos que forman parte.

El servicio de Conexión a NGN o Business Trunking es producto de la evolución de las actuales redes IP. Nace con el objeto de integrar el tráfico de voz en la red multi servicio de cliente, en respuesta a las crecientes necesidades de incorporar los contenidos multimedia. Esta red permite al cliente interconectar sus centralitas (PABX-IP) aprovechando la RPV MPLS existente.

Los equipos principales en este tipo de redes son los siguientes:
- MGW: Media Gateway, responsable de transmitir el flujo de media. Máquinas de interconexión con otras redes.
- SBC: Session Border Controler, máquinas responsables de mantener los Troncales SIP / H.323 . Se tarta de cluster de Gateway de acceso a la red NGN controlan y mantienen los troncales de cliente que conforman los Accesos Primarios Virtuales.

Funcionamiento y lógica:
Al establecerse una llamada, dado que la centralita se comunica con el AS-BT a través del SBC, este hace una manipulación numérica y agrega a la llamada en el campo de nº A los parámetros de TrunkContext y TGRP.
TrunkContext: Parámetro configurado en el AS-BT, identifica a la empresa.
TrunkGroup(TGRP): Identifica cada nodo dentro de la PBX IP. Es un identificador único y está relacionado en la aplicación con la IP del nodo. Estos parámetros identifican de manera única la empresa y PABX de la que depende el terminal que realiza la llamada. De esa forma tenemos identificada la ruta y la numeración que depende de ella.

Como redundancia a nivel de voz se ha pensado en una solución de supervivencia a través de RDSI con tarjetas SRST.

1.6.- Calidades

Al igual que en el apartado 1.4, en este apartado se distinguen las calidades contratadas a aplicar en función del tipo de sede. Es preciso indicar tal y como se ha realizado el estudio y la posterior división de los caudales en función de las necesidades de tráfico de cliente.

- Tráfico multimedia: Se marcará como trafico multimedia cualquier tráfico que tenga que ver con la telefonía IP, esto es, tráfico con origen y destino cualquiera de los CCM o cualquier tráfico dentro de la VLAN de teléfonos. Además del tráfico de voz, se marcará como tráfico multimedia cualquier tráfico relacionado con aplicaciones de video.

- Tráfico oro: En este apartado, se marcará como tráfico oro cualquier aplicación indicada por el cliente como sensible o con datos críticos y cualquier aplicación con una leve tolerancia a retardos.

- Tráfico plata: Por último, se tratará como tráfico plata todo tráfico no marcado en ninguna de las clases anteriores y el tráfico de gestión de los equipos.

A. SEDE CENTRAL

Como se ha indicado anteriormente la sede central tiene un caudal contratado de 80 Mb, de los cuales el reparto se hara de la siguiente manera:

20 Mb caudal multimedia
40 Mb caudal oro
20 Mb caudal plata

B. SEDE TIPO 1

Para las sedes Tipo 1, el caudal disponible es de 20 mb, y el reparto se realizará de la siguiente manera:

5 Mb caudal multimedia
10 Mb caudal oro
5 Mb caudal plata

C. SEDE TIPO 2

En este último tipo de sede, el caudal disponible es de 1 mb, ya que el acceso principal es ADSL y el marcado de tráfico se realiza en subida y no en bajada. Con lo cual las calidades para estos tipos de oficinas quedarían:

256 kb caudal multimedia
512 kb caudal oro
256 kb caudal plata

Dentro del estudio de las necesidades de tráfico para la adecuación de los caudales y su posterior reparto en las diferentes clases de servicio se han tenido en cuenta los siguientes aspectos.

Red de VoIP: Al diseñar la red estableciendo los servidores centrales de telefonía, Cisco Call Manager, en la sede central se requiere que ésta tenga una alta disponibilidad de caudal garantizado para tratar las llamadas así como los acceso al servidor de mensajería Unity. Además el registro de todos los teléfonos genera un tráfico, que en momentos puntuales como la apertura de las oficinas, puede crear un gran volumen. Debido a esto se decide otorgar a la sede central de un gran caudal de tráfico multimedia para atender todas estas peticiones

Red de servidores en la oficina central: El resto de oficinas debe estar haciendo continuas consultas y actualizaciones hacia ellos, lo que implica un flujo continuo con dirección oficina remota -> sede central. Es por esto que la oficina central debe tener caudales simétricos tanto en subida como en bajada, además de garantizar un caudal amplio de tráfico con marcado prioritario en red, esto es, trafico oro para todas estas aplicaciones.

Trafico de oficinas: Se estima que el tráfico de la mayoría de oficinas, dentro de la categoría 2, tanto corporativo como de acceso a internet, sea en su gran mayoría de bajada. De ahí la solución de acceso ADSL con 10 mb en bajada y 1 mb en subida.

Aplicaciones: Dentro de los aplicativos de cliente, no existe ninguna aplicación que sea sensible a retardos, con lo cual todo el tráfico corporativo de cliente se encuadrará dentro de la clase oro. Si fuera necesario por características de la aplicación tener una alta respuesta, ésta se pasaría a marcar como tráfico multimedia, junto con la VoIP.

1.7.- Equipamiento

A continuación se detallan las características técnicas de los equipos presupuestados para incluirse en cada una de las sedes de cliente, tanto a nivel de datos como de voz.

A. DATOS

- CISCO 3560

Modelo: Cisco Catalyst 3560-48PS: 48 Ethernet 10/100 ports with PoE and 4 SFP-based Gigabit Ethernet ports

Medidas: Cisco Catalyst 3560-48PS: 1.73 x 17.5 x 14.9 in. (4.4 x 44.5 x 37.8 cm)
Peso: Cisco Catalyst 3560-48PS: 13.2 lb (6.0 kg)

Rangos ambientales
- Temperatura de funcionamiento: 0 hasta 45ºC
- Temperatura de almacenamiento: -25 hasta 70ºC
- Humeda relativa de operación: 10 hasta 85%
- Altitud de operación: Hasta 3049m
- Altitud de almacenamiento: Hasta 4573m

Ruido
- ISO 7779
- Cisco Catalyst 3560-48PS: 42 dBa

Tiempo medio entre fallos - Mean Time Between Failure (MTBF)
- Cisco Catalyst 3560-48TS: 173,500 horas

Suministro de potencia maxima.
- 530W (Cisco Catalyst 3560-48PS)
- Potencia disipada: 160W, 546 BTUs per hour
- PoE: 370W

86W 293 BTU/hour

Potencia nominal
- Cisco Catalyst 3560-48PS: 0.530 kVA

Caracteristicas
- 48 Ethernet 10/100 ports and 4 SFP-based Gigabit Ethernet ports
- 1RU fixed-configuration, multilayer switch
- Enterprise-class intelligent services delivered to the network edge
- IEEE 802.3af and Cisco prestandard Power over Ethernet
- IP Services software feature set (IPS)
- Provides full IPv6 dynamic routing

- CISCO 2911

Modelo: Cisco 2911 ISR G2, 2RU

Medidas: 3.5 x 17.25 x 12 in. (88.9 x 438.2 x 304.8 mm)
Peso: 18 lb (8.2 kg)

Rangos ambientales
- Temperatura de funcionamiento: 32 hasta 104ºF (0 hasta 40ºC)
- Temperatura de almacenamiento: -40 hasta 80ºC
- Humeda relativa de operación: 5 hasta 85%
- Altitud de operación: Hasta 4000m
- Altitud de almacenamiento: Hasta 4570m

Ruido
- 58.5/70.3 dBA

Suministro de potencia maxima.
- 750W

- CISCO 1921

Modelo: CISCO1921/K9; 1RU
Medidas: 1.75 x 13.5 x 11.5 in.
Peso: 7.5 lb

Rangos ambientales
- Temperatura de funcionamiento: 0 hasta 40ºC
- Temperatura de almacenamiento: -40 hasta 70ºC
- Humeda relativa de operación: 10 hasta 85%
- Altitud de operación: Hasta 3000m
- Altitud de almacenamiento: Hasta 4570m

Ruido
- 41.99/67.22 dBA

Suministro de potencia maxima.
- 80W

Caracteristicas

2 RJ-45 onboard LAN/WAN 10/100/1000 ports 2
2 EHWIC slots
1 Doublewide EHWIC slots (use of a doublewide EHWIC slot will consume 2 EHWIC slots)
Memory (DDR2 DRAM): Default/Maximum 512 MB/512 MB
USB flash memory (internal): Default/maximum 256 MB/256 MB
1 External USB flash-memory slots (Type A)
1 USB console port (mini-Type B) (up to 115.2 kbps)
1 Serial console port (up to 115.2 kbps)
1 Serial auxiliary port (up to 115.2 kbps)

- CISCO 4500

Modelo: **Cisco Catalyst WS-C4503-E Chassis,7RU**
Medidas: 12.25 x 17.31 x 12.50 in. (31.12 x 43.97 x 31.70 cm)
Peso: 32.25 lb (14.63 kg)

Suministro de potencia maxima.
- 1667W
- Potencia disipada: 943 BTU/Hr.

Caracteristicas
Power over Ethernet (PoE)
Tarjeteria soportada Todas las tarjetas Cisco Catalyst 4000.

- CISCO 2960

Modelo: Cisco Catalyst 2960-48TT: 48 Ethernet 10/100 ports and 2 fixed Ethernet 10/100/1000 uplink ports; 1 RU
Medidas: 1.73 x 17.5 x 9.3 in. (4.4 x 44.5 x 23.6 cm)
Peso: 8.0 lb (3.6 kg)

Rangos ambientales
- Temperatura de funcionamiento: 0 hasta 45ºC
- Temperatura de almacenamiento: -25 hasta 70ºC
- Humeda relativa de operación: 10 hasta 85%
- Altitud de operación: Hasta 3049m
- Altitud de almacenamiento: Hasta 4573m

Ruido
- 40 dBa

Tiempo medio entre fallos - Mean Time Between Failure (MTBF)
- 245,213 hr

Potencia nominal
- 0.075kVA

Caracteristicas
- 48 Ethernet 10/100 ports and 2 10/100/1000TX Uplinks
- 1 RU fixed-configuration, multilayer switch
- Entry-level enterprise-class intelligent services
- LAN Base Image installed

B. VOZ

A continuación se detallan los modelos de teléfonos IP que estarán presentes en el despliegue del proyecto. Dichos modelos han sido elegidos por el cliente en base a sus necesidades de negocio y serán repartidos en base a esas mismas necesidades de manera autónoma por el cliente. Están repartidos en terminales de gama baja, terminales de gama media y terminales de gama alta.

- Cisco 7911

Caracteristicas - Funcionalidades
Iluminación de tecla de espera
Iluminación de tecla menú
Iluminación de mensajes
Indicador de espera
Display grafico
Cuatro botones de fácil acceso y barra de desplazamiento
Funciones de red
Switch Ethernet
Múltiples tonos de llamada
Control de volumen
Soporte de diferentes Codec G.711a, G.711, G.729a, G.729b, and G.729ab y iLBC
Opciones de configuratcion
Gran calidad de voz

Características de seguridad
Certificados de seguridad
Dispositivo de autenticación y cifrado de la señalización.

Especificaciones físicas y de software.
Upgrades de Firmware
Upgrades de Software
Dimensiones (H x W x D) 6.5 x 7 x 6 in. (20.3 x 17.67 x 15.2 cm)
Peso 1.9 lb (0.9 kg)

Opciones de alimentación
Cisco PoE
IEEE 802.3af PoE
Alimentación local a traves de adaptador

Rangos de temperatura
Temperatura de funcionamiento 32 hasta 104°F (0 hasta 40°C)
Humedad relativa 10 hasta 95%
Temperatura de almacenamiento 14 to 140°F (–10 hasta 60°C)

- Cisco 7942

Funcionalidades
Display de 12.5 cm y alta resolucións.
Wideband Audio
Codecs soportados G.711a, G.711µ, G.729a, G.729ab, G.722
Altavoz
Tecla de acceso directo a mensajes de voz
Tecla de directorio para acceder a llamadas recibidas, perdidas o enviadas.
Tecla de acceso rapido a ajustes
Tecla de acceso rapido a servicios
Tecla de ayuda
Tecla de altavoz, mute y auriculares
Switch Ethernet
Control de volumen
Multiples tonos de llamada
Opciones de QoS (Quality of Service)
Soporte a diferentes idiomas
Opciones de configuración

Especificaciones del producto
Dimensiones 8.2 x 10.5 x 6 in. (20.32 x 26.67 x 15.24 cm)
Peso 3.5 lb (1.6 kg)
Soporta IEEE 802.3af PoE (Clase 2).
Requiere 8.3(2) o superior
Control de compatibilidad de llamada
Varios protocolos de señalizacion

Rangos de temperatura
Temperatura de operación 32 hasta 104°F (0 hasta 40°C)
Humedad relativa 10 hasta 95%
Temperatura de almacenamiento 14 hasta 140°F (–10 hasta 60°C)

- Cisco 7970

Funcionalidades

Tecla de acceso directo a mensajes de voz
Tecla de directorio para acceder a llamadas recibidas, perdidas o enviadas.
Tecla de acceso rápido a ajustes
Tecla de acceso rápido a servicios
Display tactil de alta resolución
Tecla de altavoz, mute y auriculares
Switch Ethernet
Puerto para auriculares
Altavoz externo y puerto para micrófono
Control de volumen
Opciones flexibes de alimentacion
Multiples tonos de llamada
Soporta ptrocolo de señalización
Multiples Codecs soportados
Opciones de QoS (Quality of service)
Opciones de seguridad
Soporte a diferentes idiomas

Características de seguridad
Soporta certificados
Autenticación de dispositivo y encriptación de la señalización
Autenticación 802.1X Link Layer

Especificaciones físicas y de software.
Upgrades de Firmware
Upgrades de Software
Dimensiones (H x W x D) 9.1 x 10.5 x 6 in. (23.1 x 26.67 x 15.24 cm)
Peso 3.6 lb (1.8 kg)

Opciones de alimentación
IEEE 802.3af PoE
Cisco Pre-Standard PoE
Alimentación local mediante adaptador

Rangos de temperatura
Temperatura de operación 32 hasta 104°F (0 hasta 40°C)
Humedad relativa 10 hasta 95%
Temperatura de almacenamiento 14 hasta 140°F (-10 hasta 60°C)

Además se ofrece la posibilidad de ampliación de las características de los terminales superiores (7942 y 7970) a través de un modulo de expansión, para disponer de un mayor número de líneas o marcaciones rápidas.

- Cisco 7914 – Modulo de expansión

Botones iluminados
Botones de estado de linea
Apagado – linea disponible
Verde fijo – Linea en uso por el propio usuario

Rojo fijo – Linea en uso por otro usuario
Ambar intermitente – Llamada entrante
Verde intermitente – Llamada en espera

Especificaciones técnicas
Dimensiones: 8.0 in. x 4.75 in. x 2.0 in. (203 mm x 121 mm x 51 mm)
Peso: 0.82 lb (366 g)
Alimentación: 48 VDC, 40mA max
Temperatura de operación de LCD: 32 hasta 104ºF (0 hasta 40ºC)
Humedad relativa: 10% hasta 95%
Temperatura de almacenamiento : 12 hasta140ºF (-10 hasta 60ºC)

1.8.- Redundancia

A. DATOS

En este apartado debemos separar una posible contingencia en la oficina central y cualquier contingencia que pudiera darse en oficinas remotas, bien sea tipo 1 o tipo 2.

Respecto a la oficina central, cualquier problema a nivel de comunicaciones se resolvería mediante el protocolo HSRP configurado entre ambos equipos, bien sea lo switches de cliente o los routers, tanto de salida a internet como de acceso al resto de la MPLS. Este protocolo haría que de cara a una eventual caída de línea todo el tráfico basculara y, a través de la IP virtual configurada en el HSRP, todas las maquinas de cliente realizarían la salida a través del enlace de backup. En cuanto a la entrada de los datos a la oficina central en una situación de contingencia, el protocolo de enrutamiento de los equipos anunciaría con mejor métrica todas las redes de cliente por el enlace de backup, lo que haría bascular el tráfico en entrada de manera correcta. Hay que destacar que este tipo de redundancia es totalmente autónoma y no necesita de la intervención de ningún técnico, tanto para activarse como para volver a la situación estándar una vez superado un posible fallo en las comunicaciones.

De cara a una posible falla en las comunicaciones en las sedes remotas, tanto tipo 1 como tipo 2, la manera de proceder sería similar. Tanto en la entrada como en la salida de datos, el propio equipo se encargaría de enrutar las comunicaciones por el enlace de backup. Este proceso también se activaría y desactivaría de manera automática y sin la necesidad de ninguna intervención por parte de algún técnico. Es conveniente señalar que ante cualquier problema físico de algún equipo, bien sea en el router o en el switch de la oficina, las actuales características de la red no permiten conmutar el tráfico de ninguna manera.

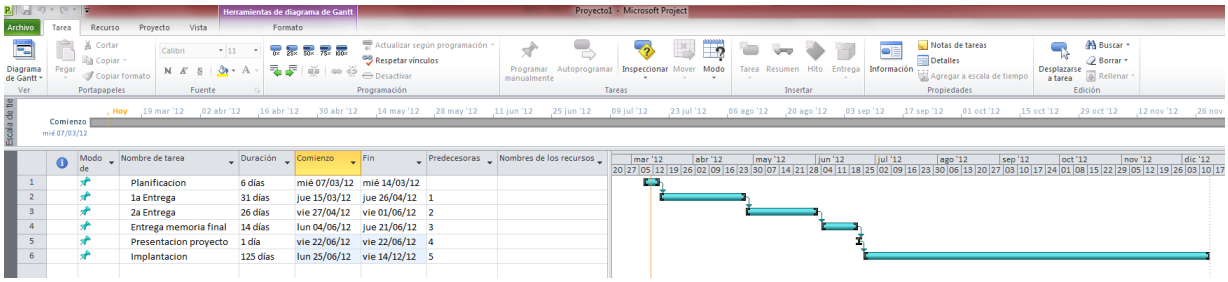
B. VOZ

En primer lugar es preciso separar entre los diferentes problemas a los que se puede enfrentar el cliente una vez se haga toda la implantación de la red. Por un lado podemos encontrar algún problema en alguno de los CCM, bien sea Publisher o Suscriber, pero éste aspecto no debe preocuparnos pues ambas maquinas están redundadas y son capaces de llevar a cabo las funciones de la otra máquina si se diera una situación de contingencia.

De cara a un posible problema de comunicaciones en una oficina remota el proceso a seguir seria el siguiente para hacer frente a una posible contingencia. Una vez los teléfonos de la oficina no tienen conectividad contra el CCM, se registran en modo supervivencia y el router de la oficina saca las llamadas a través de esta tarjeta SRST que hace de primario físico. En cuanto a las llamadas entrantes, se utiliza un desvío a nivel NGN del cabecera de la oficina afectada al número de supervivencia SRST y éste se desvía a su vez al grupo de salto de la oficina con lo cual para el usuario es transparente el modo en el que se hacen las llamadas y puede seguir funcionando con normalidad.

Es preciso destacar que tal y como se ha configurado la topología de red, no está contemplada una solución de redundancia a nivel de voz en caso de que el router o el switch de las sedes tipo 1 y 2 tenga algún problema de funcionamiento ya que están redundados a nivel de línea y no a nivel de equipo. No obstante, este supuesto tiene una probabilidad muy pequeña de darse en una situación de explotación real y dotar a todas las oficinas de un escenario de redundancia completa suponía un gran desembolso que el cliente CLIENTE S.A. no podía asumir en las circunstancias actuales.

2. DIAGRAMA DE GANT



3. ANEXO SOBRE TECNOLOGIAS

3.1.- MPLS

El Multiprotocol Label Switching (MPLS) es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. La industria ha estado buscando una solución que combine las mejores características de IP y ATM. Eso ha conducido a MPLS. El desarrollo de MPLS en las redes de los operadores de Internet es posible, ya que es transparente para el usuario.
Por otra parte, tiene grandes consecuencias para la arquitectura. MPLS ha cambiado el modelo de conmutación unicast basado en la destinación, que se había mantenido prácticamente inalterable desde el principio de Internet. A la vez, también ha impactado en la arquitectura de encaminamiento haciendo que los protocolos de encaminamiento ejecuten nuevas y más complejas tareas.

MPLS es un método de encaminamiento de paquetes en la red que usa etiquetas insertadas en el paquete IP. Las etiquetas se insertan entre la cabecera de los niveles 2 y 3 en tecnologías basadas

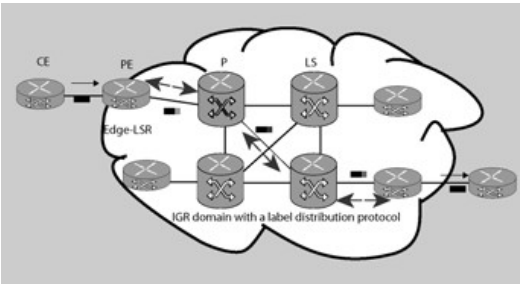
en tramas y están contenidas en el VPI/VCI en las tecnologías basadas en celdas. MPLS combina conmutación de nivel 2 y encaminamiento de nivel 3. Con conmutación de etiquetas el análisis de la cabecera nivel 3 se realiza sólo una vez, al ingresar en la red MPLS. En este punto, la cabecera nivel 3 se registra en una etiqueta de longitud fija.

La conmutación basada en etiquetas permite a los encaminadores y a los switchs ATM-MPLS tomar decisiones de envío basadas en una sencilla etiqueta, en vez de realizar una búsqueda de ruta basada en la IP destino. Los beneficios que aporta a la red IP son los siguientes:
• VPN. Los proveedores pueden crear VPN nivel 3 mediante su backbone de red para diferentes clientes, usando la misma infraestructura sin necesidad de encriptación y aplicaciones de usuario.
• Traffic engineering. Permite optimizar la utilización del ancho de banda de la red y optimizar los caminos.
• QoS. Posibilita aprovechar las características de QoS de IP y ATM.
• Integra IP y ATM.

La arquitectura MPLS está formada por dos planos:
• Control. El plano de control es responsable de unir una etiqueta con las rutas de la red (FEC) y redistribuir esta unión a los otros encaminadores MPLS. Como estamos diciendo que se une la etiqueta a una ruta de red es necesario que el encaminador tenga una tabla de encaminamiento.
Para redistribuir las etiquetas el protocolo básico es LDP (label distribution protocol). El LIB (label information base) es un mapeo de etiquetas de entrada con etiquetas de salida, junto con interfaz de salida e información de la línea. Como se ha comentado anteriormente el FEC (forwarding equivalence class) es un grupo de paquetes IP que son tratados del mismo modo. Por ejemplo, una subred destino puede corresponder a un FEC. FEC está basado en varios criterios, como pueden ser IP ToS bits, números de puerto, etc.

• Encaminamiento (forwarding). Un encaminador MPLS conmuta los paquetes IP en lugar de encaminarlos. Así, la tabla LIB se construye en el plano de control y sólo aquellas etiquetas en uso residen en label forwarding information base (LFIB). Por lo tanto, LFIB es un subconjunto de LIB. Otro componente del plano de forwarding es la tabla forwarding information base (FIB). La crea Cisco cuando usa Cisco express forwarding (CEF).

Componentes de red MPLS
Los componentes de red MPLS son los siguientes:
• CE (customer edge). Encaminador que conecta la red de usuario con el proveedor de servicio.
• PE (provider edge). Encaminador de la operadora que conecta al usuario con la red del proveedor.
• P (provider). Equipo que está en la red del proveedor y que sólo está conectado con otros equipos de la operadora



Los equipos PE y P son label switch routers (LSR). Se pueden distinguir dos tipos de LSR:
• LSR es un encaminador/switch capaz de conmutar paquetes basado en etiquetas. El CE no es un equipo LSR.

• Edge-LSR. Término más específico para los encaminadores PE. En el caso de las redes MPLS es el equipo que toma el tráfico IP no etiquetado y pone una etiqueta para enviarlo al siguiente LSR. También realiza el proceso inverso. Cuando recibe un paquete de un LSR saca la etiqueta antes de enviarlo al siguiente nodo de la red IP.

• Label switched path (LSP). Es el conjunto de LSR que el paquete ha de seguir en su flujo hacia el destino. LSP son adecuados usando varios protocolos en función de los distintos módulos de control necesarios: LDP, resource reservation protocol con traffic engineering extensions (RSVP-TE), constraint-based routed LDP (CR-LDP) o extensiones de protocolos de encaminamiento como multiprotocol BGP. El LSP puede ser considerado el camino sobre un conjunto de LSR que los paquetes que pertenecen a cierto FEC usan en su viaje para obtener su destino.

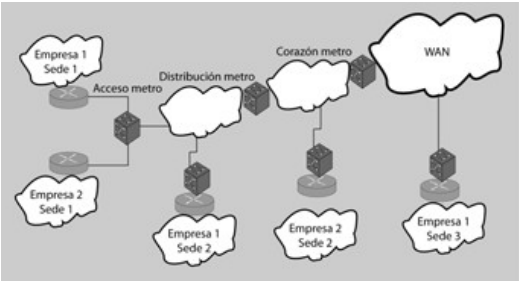
3.2.- Redes metropolitanas

La red metropolitana metropolitan area network (MAN) es un tipo de red que siempre se ha clasificado como una red que está entre LAN y WAN. Una red MAN por el hecho de tener órdenes de magnitud cubriría un área que puede ir de 5 a 50 km, aunque estos valores son siempre relativos.

La red metro es el primer tramo de la red que conecta usuarios finales y empresas a la red WAN. La parte de red metro que llega al usuario final se llama "la última milla", con el fin de indicar que es el último tramo de la red portadora.

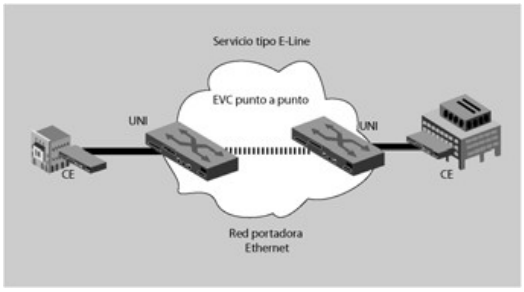
El concepto MAN no es nuevo. Surge en torno a los años noventa. En aquella época los anillos TDM (time division multiplexing) formaban la red MAN con amplificadores ópticos para cumplir los objetivos de distancia. A mediados de los años noventa fue ATM la tecnología dominante en las redes MAN, por el hecho de que existía la promesa de que ATM sería la tecnología que permitiría la convergencia de datos, voz y vídeo. Además, ATM permitía usar ATM por encima del anillo SDH. El problema consistió en que mientras SDH fue incrementando su estructura, ATM no consiguió introducirse como la solución empleada por el usuario final.

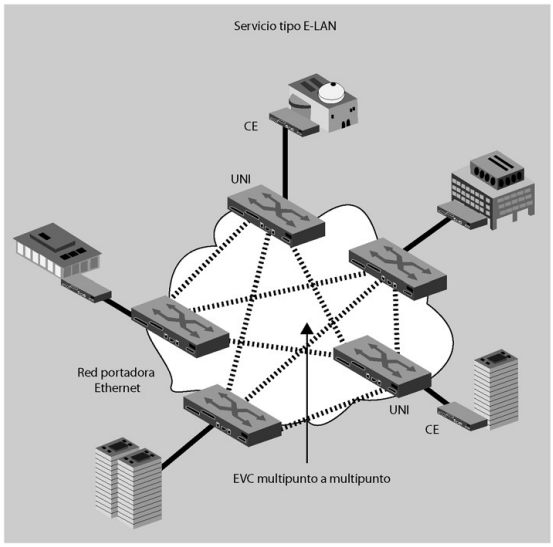
Si miramos en perspectiva la red metro, se puede ver que está básicamente dividida en tres partes:
1) Acceso metro (access metro). Este segmento constituye la última milla, que es la parte que tocaría al usuario final.
2) Distribución metro (metro edge). Este segmento constituye el primer nivel de la agregación metro. Las conexiones que salen de los edificios son agregadas a la CO en conexiones más grandes que sucesivamente son transportadas mediante la red metro o la red WAN.
3) Corazón metro (metro core). Este segmento constituye el segundo nivel de agregación, donde las CO lindantes son agregadas a una CO central. A la vez, las CO centrales se conectan con otras, de modo que forman un corazón metro desde donde el tráfico es enviado mediante la WAN.



Como se ha dicho, Ethernet es una tecnología sobradamente extendida a un precio adecuado y, a la vez, la mayoría de dispositivos de telecomunicaciones disponen de interfaz Ethernet. Las interfaces

pueden ir a velocidades de 10/100/1.000 Mbps y desde el año 2002 está ratificado por el IEEE el estándar a 10 Gbps.
En entornos metropolitanos Ethernet posee un gran potencial, teniendo en cuenta la capacidad que tiene de incrementar la red a un coste efectivo y el hecho de que ofrece la posibilidad de introducir nuevos servicios de manera escalable, sencilla y flexible. Algunos proveedores están extendiendo Ethernet a la red WAN.
Desde el punto de vista empresarial Ethernet tiene dos servicios de aplicación clave: por una parte, conectividad con la red Internet y, por otra, la conectividad entre sedes geográficamente separadas mediante extensiones LAN.
Los enlaces normalmente son punto a punto. Los nodos pueden ser o switchs o encaminadores, en función de su localización.
Otro aspecto importante dentro de los servicios Ethernet metropolitanos son las conexiones virtuales Ethernet (EVC). Estas EVC conectan dos o más sedes de usuario (UNI). Los servicios Ethernet, en función de la topología de EVC, se pueden clasificar en:
• E-Line: enlaces punto a punto
• E-LAN: enlaces multipunto a multipunto





Para el proyecto que nos ocupa, la opción elegida es la de E-LAN, enlaces multipunto a multipunto.

3.3.-Redes privadas virtuales

Una red privada virtual (VPN, virtual private network) es una red privada construida dentro de una infraestructura de red pública, tal como la red mundial de Internet. Las empresas pueden usar redes privadas virtuales para conectar en forma segura oficinas y usuarios remotos a través de accesos a Internet económicos proporcionados por terceros, en vez de costosos enlaces WAN dedicados o enlaces de marcación remota de larga distancia.

Las organizaciones pueden usar redes privadas virtuales para reducir los costos de ancho de banda de redes WAN, y a la vez aumentar las velocidades de conexión a través de conectividad a Internet de alto ancho de banda, tal como DSL, Ethernet o cable.

Las redes privadas virtuales proporcionan el mayor nivel posible de seguridad mediante seguridad IP (IPsec) cifrada o túneles VPN de Secure Sockets Layer (SSL) y tecnologías de autenticación. Estas tecnologías protegen los datos que pasan por la red privada virtual contra accesos no autorizados. Las empresas pueden aprovechar la infraestructura estilo Internet de la red privada virtual, cuya sencillez de abastecimiento permite agregar rápidamente nuevos sitios o usuarios. También pueden aumentar drásticamente el alcance de la red privada virtual sin expandir significativamente la infraestructura.

Las redes privadas virtuales extienden la seguridad a los usuarios remotos

Las redes VPN SSL y VPN IPsec se han convertido en las principales soluciones de redes privadas virtuales para conectar oficinas remotas, usuarios remotos y partners comerciales, porque:

Proporcionan comunicaciones seguras con derechos de acceso adaptados a usuarios individuales, tales como empleados, contratistas y partners

Aumentan la productividad al ampliar el alcance de las redes y aplicaciones empresariales

Reducen los costos de comunicación y aumentan la flexibilidad

Los dos tipos de redes virtuales privadas cifradas:

VPN IPsec de sitio a sitio: Esta alternativa a Frame Relay o redes WAN de línea arrendada permite a las empresas extender los recursos de la red a las sucursales, oficinas en el hogar y sitios de los partners comerciales.

VPN de acceso remoto: Esto extiende prácticamente todas las aplicaciones de datos, voz o video a los escritorios remotos, emulando los escritorios de la oficina central. Las redes VPN de acceso remoto pueden desplegarse usando redes VPN SSL, IPsec o ambas, dependiendo de los requisitos de implementación.

Sobre lo comentado anteriormente, y en el ámbito de este proyecto se define el servicio VPN IP como un servicio de interconexión de redes locales sobre infraestructura IP basada en tecnología MPLS. El servicio permite la creación de redes privadas virtuales sobre dicha infraestructura manteniendo las mismas prestaciones que si fuera una red privada, reduciendo costes y aumentando rendimiento.

El servicio es adecuado para el cliente que necesite una topología de red altamente mallada "todos con todos" y de diferenciar el tratamiento de los distintos tráficos que realiza.

Las principales características de este servicio son las siguientes:
-Conexión permanente con accesos punto a punto o ADSL.
-Tratamiento diferenciado del tráfico según su prioridad.
-Permite la utilización de direccionamiento IP público o privado, o de protocolos distintos de IP.
-Conectividad de "todos con todos". Topología totalmente mallada que por medio de la tecnología MPLS se consigue mayor eficiencia de sus comunicaciones con tiempos de retardo mínimos.
-Acceso a Internet de las delegaciones de la red del cliente.
La salida a Internet desde la VPN-IP, se soporta sobre el Servicio de acceso a internet centralizado, proporcionando a su red privada virtual de salida a Internet gestionada y segura desde la Red IP, con lo cual, no tiene que sobredimensionar ninguno de sus accesos para dar salida a Internet a cada una de las delegaciones que componen la RPV. Se contratará un Caudal Agregado a Internet, para toda la RPV y estará compartido por todas las delegaciones de manera equitativa de manera proporcional a la velocidad del acceso de cada sede.

3.4.-Voz sobre IP

La voz-ip es una tecnología que permite encapsular la voz en paquetes para poder ser transportados sobre redes de datos sin necesidad de disponer de los circuitos conmutados convencionales. La telefonía IP no utiliza circuitos físicos para la conversación, sino que envía múltiples conversaciones a través del mismo canal (circuito virtual) codificadas en paquetes y en flujos independientes. Cuando se produce un silencio en una conversación, los paquetes de datos de otras conversaciones pueden ser transmitidos por la red, lo que implica un uso más eficiente de la misma.

Una red de Voz sobre IP presenta las siguientes características:
Permite el control del tráfico de la red, por lo que se disminuyen las posibilidades de que se produzcan caídas importantes en el rendimiento de las redes de datos.

Proporciona el enlace a la red telefónica tradicional.

Al tratarse de una tecnología soportada en IP presenta las siguientes ventajas adicionales:

Es independiente del tipo de red física que lo soporta. Permite la integración con las grandes redes de IP actuales.

Es independiente del hardware utilizado.

Permite ser implementado tanto en software como en hardware, con la particularidad de que el hardware supondría eliminar el impacto inicial para el usuario común.

Dentro de los protocolos de funcionamiento, podemos encontrar los siguientes:
SIP (Session Initiation Protocol)

SIP son las siglas en inglés del Protocolo para Inicio de Sesión, siendo un estándar desarrollado por el IETF, identificado como RFC 3261, 2002. SIP es un protocolo de señalización para establecer las llamadas y conferencias en redes IP. El inicio de la sesión, cambio o término de la misma, son independientes del tipo de medio o aplicación que se estará usando en la llamada; una sesión puede incluir varios tipos de datos, incluyendo audio, video y muchos otros formatos

H.323
H.323 fue el primer estándar internacional de comunicaciones multimedia, que facilitaba la convergencia de voz, video y datos. Fue inicialmente construido para las redes basadas en conmutación de paquetes, en las cuales encontró su fortaleza al integrarse con las redes IP, siendo un protocolo muy utilizado en VoIP.

En nuestro caso, el elegido para el proyecto será SIP.

Otro elemento a tener en cuenta, es que en el diseño de la solución de voz sobre ip, no será necesaria la utilización de gateways ya que se ha diseñado una implementación de voz sobre ip mediante primarios virtuales (NGN) con lo cual la conexión a la red telefónica básica (PSTN) se hará de manera virtual en primarios físicos responsabilidad del proveedor. Esto supone un ahorro ya que el cliente no necesita disponer de primarios físicos en todas y cada una de sus oficinas para dotar de conexión a su red de voz sobre ip con el resto de la PSTN.

3.5.-Encaminamiento de llamadas

LLAMADAS ENTRANTES DESDE LA RED PÚBLICA (NGN)
Las llamadas entrantes, a través de NGN se encaminarán hacia la sede central y de ahí a su destino final estableciéndose la comunicación pertinente entre la extensión IP de la sede y el llamante a través de Translation Patterns configurados en CCM.

LLAMADAS SALIENTES A LA RED PÚBLICA (NGN)
Desde cualquier extensión IP de la red del cliente CLIENTE S.A. que tenga permisos de salida se podrá hacer cualquier tipo de comunicación con el exterior a través de los primarios virtuales configurados en la red NGN.

LLAMADAS INTERNAS
Todos los terminales IP tendrán permisos de llamadas internas para comunicarse con cualquier otra extensión de la red sin coste alguno para el cliente CLIENTE S.A.

3.6.-Cisco Call Manager - CCM

De manera global, se entiende Cisco Unified Communications Manager (CUCM) o simplemente Cisco Call Manager (CCM) como un software basado en un sistema para el tratamiento de llamadas y telefónica sobre IP del fabricante Cisco.

Sobre su modo de funcionamiento, CCM rastrea los posibles componentes de VoIP activos en la red, tales como teléfonos, GW's, mensajería de voz, etc... A menudo utiliza como protocolo SCCP para la señalización de parámetros. Además utiliza SIP o H323 para endosar la señalización de llamadas a los GW's

4. ALCANCE DEL PROYECTO

A continuación se adjunta el listado de oficinas, facilitadas por el cliente CLIENTE S.A. que están dentro del alcance de este proyecto.

DENOMINACIÓN	TIPO SEDE	IP LAN
Sede Central Madrid	SEDE CENTRAL	10.100.0.0/23
Sede Norte Barcelona	TIPO 1	10.100.2.0/24
Sede Sur Sevilla	TIPO 1	10.100.3.0/24
Albacete	TIPO 2	10.100.4.0/24
Alicante	TIPO 1	10.100.5.0/24
Almería	TIPO 2	10.100.6.0/24
Ávila	TIPO 2	10.100.7.0/24
Badajoz	TIPO 2	10.100.8.0/24
Bilbao	TIPO 1	10.100.9.0/24
Burgos	TIPO 2	10.100.10.0/24
Cáceres	TIPO 2	10.100.11.0/24
Cádiz	TIPO 2	10.100.12.0/24
Castellón	TIPO 2	10.100.13.0/24
Ceuta	TIPO 2	10.100.14.0/24
Ciudad Real	TIPO 2	10.100.15.0/24
Córdoba	TIPO 2	10.100.16.0/24
Cuenca	TIPO 2	10.100.17.0/24
Gerona	TIPO 2	10.100.18.0/24
Granada	TIPO 2	10.100.19.0/24
Guadalajara	TIPO 2	10.100.20.0/24
Huelva	TIPO 2	10.100.21.0/24
Huesca	TIPO 2	10.100.22.0/24
Jaén	TIPO 2	10.100.23.0/24
La Coruña	TIPO 1	10.100.24.0/24
León	TIPO 2	10.100.25.0/24
Logroño	TIPO 2	10.100.26.0/24
Lugo	TIPO 2	10.100.27.0/24
Lérida	TIPO 2	10.100.28.0/24
Madrid	TIPO 1	10.100.29.0/24
Málaga	TIPO 1	10.100.30.0/24
Melilla	TIPO 2	10.100.31.0/24
Murcia	TIPO 2	10.100.32.0/24
Orense	TIPO 2	10.100.33.0/24
Oviedo	TIPO 2	10.100.34.0/24
Palencia	TIPO 2	10.100.35.0/24
Palma de Mallorca	TIPO 1	10.100.36.0/24
Las Palmas de Gran Canaria	TIPO 2	10.100.37.0/24
Pamplona	TIPO 2	10.100.38.0/24
Pontevedra	TIPO 2	10.100.39.0/24
Salamanca	TIPO 2	10.100.40.0/24
San Sebastián	TIPO 1	10.100.41.0/24
Santa Cruz de Tenerife	TIPO 1	10.100.42.0/24
Santander	TIPO 2	10.100.43.0/24
Segovia	TIPO 2	10.100.44.0/24
Soria	TIPO 2	10.100.45.0/24
Tarragona	TIPO 2	10.100.46.0/24
Teruel	TIPO 2	10.100.47.0/24
Toledo	TIPO 2	10.100.48.0/24
Valencia	TIPO 1	10.100.49.0/24
Valladolid	TIPO 1	10.100.50.0/24
Vitoria	TIPO 2	10.100.51.0/24

Zamora	TIPO 2	10.100.52.0/24
Zaragoza	TIPO 1	10.100.53.0/24

En resumen, tenemos 1 sede central, 13 sedes tipo 1 y 39 sedes tipo 2.

5. VALORACION ECONOMICA

A continuación se detalla el desglose económico que supone la implantación del siguiente proyecto de comunicaciones.

Accesos FIBRA				
CONCEPTO	**UNID.**	**CAUDAL**	**CUOTA DE ALTA**	**CUOTA MENSUAL**
Sede Central Madrid	2	80 Mb	-	10000€
Sede Norte Barcelona	1	20 Mb	-	2000€
Sede Sur Sevilla	1	20 Mb	-	2000€
Alicante	1	20 Mb	-	2000€
Bilbao	1	20 Mb	-	2000€
La Coruña	1	20 Mb	-	2000€
Madrid	1	20 Mb	-	2000€
Málaga	1	20 Mb	-	2000€
Palma de Mallorca	1	20 Mb	-	2000€
San Sebastián	1	20 Mb	-	2000€
Sta. Cruz de Tenerife	1	20 Mb	-	2000€
Valencia	1	20 Mb	-	2000€
Valladolid	1	20 Mb	-	2000€
Zaragoza	1	20 Mb	-	2000€
Cisco 3845	2	-	600€	600€
Cisco 4500	2	-	800€	800€
Cisco 2911	13	-	400€	400€
Cisco 2960	13	-	600€	600€
			15800€	**51800€**
TOTAL				**67600€**

Accesos ADSL – VPN IP				
CONCEPTO	**UNID.**	**CAUDAL**	**CUOTA DE ALTA**	**CUOTA MENSUAL**
Albacete	1	10Mb-1Mb	-	500€
Almería	1	10Mb-1Mb	-	500€
Ávila	1	10Mb-1Mb	-	500€
Badajoz	1	10Mb-1Mb	-	500€
Burgos	1	10Mb-1Mb	-	500€
Caceres	1	10Mb-1Mb	-	500€
Cadiz	1	10Mb-1Mb	-	500€
Castellon	1	10Mb-1Mb	-	500€
Ceuta	1	10Mb-1Mb	-	500€
Ciudad Real	1	10Mb-1Mb	-	500€
Cordoba	1	10Mb-1Mb	-	500€
Cuenca	1	10Mb-1Mb	-	500€
Gerona	1	10Mb-1Mb	-	500€
Granada	1	10Mb-1Mb	-	500€
Guadalajara	1	10Mb-1Mb	-	500€
Huelva	1	10Mb-1Mb	-	500€
Huesca	1	10Mb-1Mb	-	500€
Jaén	1	10Mb-1Mb	-	500€
León	1	10Mb-1Mb	-	500€
Logroño	1	10Mb-1Mb	-	500€
Lugo	1	10Mb-1Mb	-	500€
Lérida	1	10Mb-1Mb	-	500€
Melilla	1	10Mb-1Mb	-	500€
Murcia	1	10Mb-1Mb	-	500€
Orense	1	10Mb-1Mb	-	500€
Oviedo	1	10Mb-1Mb	-	500€
Palencia	1	10Mb-1Mb	-	500€
Las Palmas de Gran Canaria	1	10Mb-1Mb	-	500€
Pamplona	1	10Mb-1Mb	-	500€
Pontevedra	1	10Mb-1Mb	-	500€
Salamanca	1	10Mb-1Mb	-	500€
Santander	1	10Mb-1Mb	-	500€
Segovia	1	10Mb-1Mb	-	500€
Soria	1	10Mb-1Mb	-	500€
Tarragona	1	10Mb-1Mb	-	500€
Teruel	1	10Mb-1Mb	-	500€
Toledo	1	10Mb-1Mb	-	500€
Vitoria	1	10Mb-1Mb	-	500€
Zamora	1	10Mb-1Mb	-	500€
Cisco 2811	39	-	300€	300€
Cisco 2960	39	-	600€	600€
			35100€	**54600€**
TOTAL				**89700€**

Servicio Acceso Internet				
CONCEPTO	**UNID.**	**CAUDAL**	**CUOTA DE ALTA**	**CUOTA MENSUAL**
Sede Central Madrid	2	20 Mb		6000€
Cisco 2911	2	-	400€	400€
			800€	**12800€**
TOTAL				**13600€**

CONCEPTO	**UNID.**	**CUOTA DE ALTA**	**CUOTA MENSUAL**
CCMS	1	2500€	2500€
CCMP	1	2500€	2500€
UNITY	1	1700€	1700€
Cisco 7911	89	200€	-
Cisco 7942	71	350€	-
Cisco 7970	18	450€	-
Cisco 7914	13	150€	-
		59400€	**6700€**
TOTAL			**66100€**

Queda fuera del alcance del cuadro anterior la tarificación de las llamadas por medio de los primarios virtuales, ya que se ha establecido un acuerdo sin cuota fija mensual, el cliente CLIENTE S.A. sólo facturará en base al consumo por segundos del mes anterior.

El reparto de teléfonos se ha hecho en base a las necesidades de negocio del cliente CLIENTE S.A.

6. ANEXO SOBRE PROTOCOLOS

4.1.-BGP

El BGP o Border Gateway Protocol es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos. Por ejemplo, los ISP registrados en Internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP.

Entre los sistemas autónomos de los ISP se intercambian sus tablas de rutas a través del protocolo BGP. Este intercambio de información de encaminamiento se hace entre los routers externos de cada sistema autónomo. Estos routers deben soportar BGP. Se trata del protocolo más utilizado para redes con intención de configurar un Exterior Gateway Protocol.

La forma de configurar y delimitar la información que contiene e intercambia el protocolo BGP es creando lo que se conoce como sistema autónomo. Cada sistema autónomo (AS) tendrá conexiones o, mejor dicho, sesiones internas (iBGP) y además sesiones externas (eBGP).

El protocolo de gateway fronterizo (BGP) es un ejemplo de protocolo de gateway exterior (EGP). BGP intercambia información de encaminamiento entre sistemas autónomos a la

vez que garantiza una elección de rutas libres de bucles. Es el protocolo principal de publicación de rutas utilizado por las compañías más importantes de ISP en Internet.

Sin entrar en demasiadas complejidades técnicas, se ha elegido este protocolo ya que se trata de un protocolo de estado duro que no necesita enviar actualizaciones periódicas si no hay cambios en su tabla de rutas, lo que redunda en un % superior de disponibilidad de la red, y porque permite conocer todas las redes de la red de cliente desde cualquier de las oficinas eliminando procesos de routing en la red del proveedor.

Como se comenta anteriormente, el CE, customer edge, equipo de cliente, mantendrá una sesión BGP contra el PE o extremo del proveedor, donde se intercambiaran todas las rutas disponibles para la VPN de cliente.

4.2.-HSRP

El Hot Standby Router Protocol es un protocolo propiedad de CISCO que permite el despliegue de routers redundantes tolerantes a fallos en una red. Este protocolo evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers.

Se ha pensado en la implementación en este proyecto para la sede central del protocolo HSRP ya que todo el equipamiento va a ser Cisco, que a su vez es propietario de este protocolo. Si el cliente optara en un futuro por cambiar el fabricante de sus equipos, es bueno señalar que podrían seguir teniendo esta solución de redundancia a través del protocolo VRRP que es similar en funcionacmiento al HSRP pero que funciona sobre equipos Teldat o Juniper.

Dentro del funcionamiento de este protocolo, se estable un router principal que tendrá una prioridad superior a la prioridad habitual, por defecto 100. Asimismo en el equipo principal se configurara un evento que una vez ocurra, un fallo en la línea principal por ejemplo, haga que la prioridad se decremente en X unidades. Convenientemente estará el backup configurado con una prioridad que la hará coger el testigo del principal y pasar a ser router master.

Una vez se solucione el problema en la línea, también deberá estar configurado una linea de comandos que permita al router principal volver a retomar el testigo como router maestro.

4.3.-SNMP

Se define en este punto el protocolo SNMP, Protocolo Simple de Administración de Red o SNMP (del inglés Simple Network Management Protocol) para facilitar al cliente la obtención de medidas de tráfico, estadísticas o incluso graficas de todos y cada uno de los dispositivos que integraran su red de comunicaciones.

En la actualidad existen multitud de herramientas que permiten obtener graficas de rendimiento sobre una red telemática. En nuestro proyecto se ha pensado en una solución de MRTG, MRTG (Multi Router Traffic Grapher) es una herramienta, escrita en C y Perl, que se utiliza para supervisar la carga de tráfico de interfaces de red. MRTG genera un

informe en formato HTML con gráficas que proveen una representación visual de la evolución del tráfico a lo largo del tiempo.

Para realizar estas gráficas, se basa en consultas realizadas mediante SNMP.

Por SNMP entendemos el protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas. Se compone de 3 elementos clave, Dispositivos administrados, Agentes y Sistemas administradores de red (Network Management Systems, NMS's).

Los dispositivos administrados son supervisados y controlados usando cuatro comandos SNMP básicos: lectura, escritura, notificación y operaciones transversales.

El comando de lectura es usado por un NMS para supervisar elementos de red. El NMS examina diferentes variables que son mantenidas por los dispositivos administrados.

El comando de escritura es usado por un NMS para controlar elementos de red. El NMS cambia los valores de las variables almacenadas dentro de los dispositivos administrados.

Una vez hecha la introducción al protocolo es preciso señalar que se ha pensado en incluir, para facilidad de cliente, una configuración estándar en todos y cada uno de los routers de la VPN del cliente CLIENTE S.A. que permita a éste monitorizar su red en tiempo real, con el fin de realizar el control del tráfico, auditoria, estudios de anchos de banda, cuellos de botella y otros problemas o mejoras cualquieras en la red.

7. BIBLIOGRAFIA

Cisco.com
Wikipedia.org
Materiales UOC – Redes y Servicios