INSTITUTO POLITECNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN

IMPLEMENTACIÓN DE TELEFONÍA IP SOBRE VPN

T E S I N A

SEMINARIO DE TITULACIÓN: INTERCONECTIVIDAD Y SEGMENTACIÓN DE REDES DE ALTA VELOCIDAD

VIGENCIA: FNS 5052005/14/2008

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMUNICACIONES Y ELECTRÓNICA
PRESENTAN:

GARCIA HINOJOSA ISRAEL
LEAL CORTES SERGIO
LOPEZ MORALES EDY SAMUEL
SAUCEDO DOMINGUEZ JORDAN DAVID

ASESORES: **DR. GABRIEL SÁNCHEZ PÉREZ**
M.en C. LUIS CARLOS CASTRO MADRID.

MEXICO, D.F **Noviembre de 2008**

AGRADECIMIENTOS:

GARCIA HINOJOSA ISRAEL

A mis padres por todo el apoyo que me han brindado durante toda mi carrera, ya que por ellos he alcanzado a cumplir mis metas. Por esto y más les agradezco mucho y comparto con ellos este triunfo.

LEAL CORTES SERGIO

A esas mujeres que con su ejemplo y consejos me han demostrado su amor, y me han enseñado el significado de la fe y la esperanza, les agradezco infinitamente. Es por esto y por muchas otras cosas que les dedico este triunfo.

Gracias

LOPEZ MORALES EDY SAMUEL

A mis padres, Samuel López y Raquel Morales, que con su cariño, sacrificios y esmeros, hicieron posible la culminación de este logro, si volviera a nacer me encantaría ser su hijo nuevamente, los amo con todo mi corazón.

A mis hermanos, Wendy, Mónica, Fanny, Elizabeth, Álvaro, Arturo y Raymundo por darme la oportunidad de ser su amigo, además de brindarme su apoyo incondicional.

A mis sobrinos, Donovan, Axel, y Bryan por llenar de felicidad, alegría todos mis momentos.

Al amor de mi vida, Lorena Alejandra Barajas, por ser la inspiración y el motor de cambio para ser una persona de bien, que ha estado en los buenos y malos momentos, apoyándome a conseguir este logro tan importante.

A mis amigos, Jerardo Rodríguez Coroy, Arcadio Calderón, Segundo Hernández, Juan Manuel Quiñones, Sergio Leal, Israel García, Jordán Saucedo, Constantino Ruiz, Juan Carlos Mejía, por ser tan incondicionales y ser el tesoro más valioso que tengo.

Y con un cariño significativo al Instituto Politécnico Nacional, por darme las herramientas necesarias para llevar a cabo la tarea más importante, compartir los conocimientos adquiridos a la sociedad y mi país.

SAUCEDO DOMINGUEZ JORDAN DAVID

Con este documento cierro un círculo en mi vida Profesional.
Sigo avanzando orgulloso de ser un egresado del IPN.
Agradezco la invitación a formar parte de este gran equipo de trabajo, y estar dentro de un muy interesante proyecto.

Agradezco el apoyo que he recibido por la gente que estimo, que incondicionalmente esta a mi lado, demostrándome como salir adelante y llegando a sus metas, adaptándose, son personas dignas de mi admiración, respeto y cariño. Son una parte muy importante de este logro.

Comparto este proyecto con ustedes.

“Uno es dueño de su propio destino, vive cada momento, disfruta cada experiencia,
Solo pregúntate qué harías sin miedo de realizar las cosas, traza tus metas, obsérvate en ellas, de verdad, lo qué te propongas con esmero y dedicación tendrá su recompensa… ”

INDICE

CAPITULO 4 OPCIONES PARA TRANSPORTAR VOZ.

CAPITULO 5 IMPLEMENTACIÓN DE TELEFONÍA IP SOBRE VPN

INTRODUCCIÓN

IMPLEMENTACIÓN DE TELEFONÍA IP SOBRE VPN

La masificación de la gran red de redes, Internet, produjo un acercamiento de los individuos y organizaciones, en lo que a las comunicaciones respecta. De repente, enviar una carta o un FAX a otro lugar, se tornó más lento y más caro que enviar un mensaje de correo electrónico, el tener una conferencia telefónica se convirtió en una actividad obsoleta, a la par de una video conferencia ó una simple charla por cualquier otro servicio de chat, todo esto a través de Internet.

A medida que Internet se popularizó, las empresas comenzaron a ver este medio como algo que les permitía enviar y recibir información de todo tipo de manera rápida y económica. Pero cuando uno habla de información, normalmente no clasifica esa información, y así como Internet es masiva, es también insegura en lo que respecta a privacidad durante el tránsito de la información.
¿Qué se puede hacer con servicios, como por ejemplo conexión a base de datos, a servidores web internos, o cualquier otro servicio que exista o esté por existir?
La solución a esta problemática requiere de un medio de transferencia seguro, que se establezca sobre el medio inseguro pero extremadamente barato y disponible como es Internet. Este medio proveería lo necesario para que las conexiones se realicen de forma transparente y segura. A este medio se lo denomina VPN, o Red Privada Virtual.
Una red privada y virtual tiene, como su nombre lo indica, dos componentes:
Virtual
Es virtual porque la conexión que se establece no es una conexión de red física como se acostumbra a configurar, sino que se crean interfaces de red virtuales de tal manera de engañar a las aplicaciones que se posee una red adicional, y de esta manera poder utilizarlas sin ningún requerimiento extra sobre estos tipos de conexiones.
Privada
De nada sirve simular una conexión de red solamente, en lo que respecta a privacidad, es necesario además agregar un componente de cifrado de algún tipo, que se realice al nivel de la capa de red, en la capa inmediata superior a la interfaz virtual, de modo tal que sólo pueda ser descifrada la información al otro lado de la conexión, y por lo tanto, mantener la privacidad de los datos enviados y recibidos.

Por otra parte, el crecimiento y fuerte implantación de las redes IP, tanto en local como en remoto, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización de tráfico, protocolos de transmisión en tiempo real, así como el estudio de nuevos estándares que permitan la calidad de servicio en redes IP, han creado un entorno donde es posible transmitir telefonía sobre IP lo que no significará en modo alguno la desaparición de las redes telefónicas modo circuito, sino que habrá, al menos temporalmente, una fase de coexistencia Si a todo lo anterior, se le suma el fenómeno Internet, junto con el potencial ahorro económico que este tipo de tecnologías puede llevar acarreado, la conclusión es clara: El VoIP (Protocolo de Voz Sobre Internet - Voice Over Internet Protocol) es un tema estratégico para las empresas.

En este proyecto se realizara una conexión entre equipos a través de VPN y realizaremos VoIP, mediante un software llamado softphone.

Un Softphone (en inglés combinación de Software y de Telephone) es un software que hace una simulación de teléfono convencional por computadora. Es decir, permite usar la computadora para hacer llamadas a otros softphones o a otros teléfonos convencionales.

En el presente documento se muestra una aplicación con las soluciones propuestas, dentro de la empresa Distribuidora Biogama S. A. de C. V.
Empresa mexicana encargada de proveer equipo y reactivos médicos a diferentes laboratorios y hospitales del país,

Tiene aproximadamente seis años de vida en los cuales se ha desarrollo de una manera muy eficaz, teniendo como clientes al sector privado y desde hace tres años en el sector publico, ganando diversas licitaciones, es por esto que se ve a la necesidad de replantear sus sistemas de comunicaciones para hacerle frente a los nuevos retos que se le presenten.

En la empresa se cuenta con aproximadamente 30 empleados, los cuales están distribuidos en diferentes áreas; administrativas y operativas.

La distribución del personal se distribuye de la siguiente manera, 15 usuarios ubicados en las oficinas que se encargan de la parte administrativa, ellos cuentan con servicios de voz y datos. En la parte operativa hay 10 personas, que desempeñan las actividades de recolección y entrega de los productos, además cuentan con 5 vendedores distribuidos en varios estados de la republica

OBJETIVO:

Implementación VoIP a través de VPN, sobre la infraestructura de una empresa.

PROBLEMÁTICA:

En la actualidad las empresas cuentan con información no centralizada y generan gastos excesivos en comunicación tanto de voz como al igual de datos.

JUSTIFICACIÓN:

- Comunicación directa, entre las oficinas de los usuarios, en su computadora
- Fácil uso, extensión de 4 dígitos de la red telefónica de la empresa
- Fácil implementación sobre infraestructura de Internet instalada
- Ahorros económicos en los tiempos de llamadas y servicio de largas distancias
- Mantenimiento económico y soporte remoto sencillo
- Almacenamiento de información de manera segura a través de un túnel en Internet

ALCANCE:

-Generar una VPN (Red Privada Virtual) con equipo CISCO
-La instalación y configuración del Cliente VPN de Cisco Systems, aplicación que permite acceder a la Red Privada Virtual que se ha creado para dar servicio de telefonía IP de forma segura y confidencial con los usuarios que utilizaran este servicio solo en sus computadoras portátiles y fuera de sus oficinas
-La instalación y configuración del softphone dentro del equipo portátil, aplicación con la que realizaremos la comunicación de voz IP

CAPITULO 1 INTRODUCCIÓN A LAS REDES.

1.1.- FUNDAMENTOS DE UNA PC.

Debido a que las computadoras son piezas importantes dentro de una red, es importante ser capaz de reconocer y denominar los componentes básicos de una PC. Se debe pensar en los componentes internos de una PC como en los dispositivos de una red, todos ellos conectados al bus del sistema. En cierta forma, una PC es una pequeña red de computadoras.

Muchos dispositivos de una red, como los routers y los switches, son en sí mismo computadoras de propósito específico y tienen muchas de las partes habituales de las PC normales. Para emplear la computadora como un medio fiable para obtener información, debe funcionar correctamente. Debe estar en disposición de poder reconocer, nombrar y manifestar el propósito de los componentes de una PC (esta información también puede aplicarse a una portátil).

1.2.- COMPONENTES ELECTRÓNICOS.

Los componentes electrónicos son únicos en cuanto están diseñados para conducir o transmitir datos o señales de forma electrónica. Muchos de los componentes electrónicos se encuentran en la placa madre y en las tarjetas de expansión que se conectan a ella. A continuación se tiene algunas de las partes que normalmente se pueden encontrar en los componentes electrónicos:

- Transistor.
- Circuito Integrado (IC, *Integrated Circuit*).
- Resistencia.
- Condensador.
- Conector.
- Diodo electroluminiscente (LED, *Light Emitting Diode*).

1.3.- COMPONENTES DE UNA PC.

Normalmente se piensa en los componentes de una PC como en partes empaquetadas o añadidas que proporcionan una funcionalidad adicional a una PC. Contrastan con los componentes electrónicos vitales necesarios en toda PC. Entre los componentes de una PC podemos citar las unidades de disco, la memoria, los discos duros, los procesadores y la fuente de alimentación. A continuación se muestran algunos de los componentes más comunes en una PC.

- Placa de circuito impreso (PCB, Printed Circuit Board).
- Unidad de CD-ROM.
- Unidad central de procesamiento *(CPU, Central Processing Unit).*
- Unidad de disco flexible.
- Unidad de disco duro.
- Microprocesador.
- Placa madre.
- Bus.

- Memoria de acceso aleatorio *(RAM, Random-Access Memory).*
- Memoria de sólo lectura *(ROM, Read-Only Memory).*
- Ranura (o spot) de expansión.
- Unidad del sistema.
- Fuente de alimentación.

1.4.- COMPONENTES DE LA PLACA MADRE.

La placa madre es la tarjeta de la computadora. Es vital porque es el centro neurálgico del sistema de computación. Todo lo demás va conectado a ella, esta controlado por ella y depende de ella para poder comunicarse con otros dispositivos del sistema. La siguiente lista describe distintos componentes de la placa madre:

- Plano trasero.
- Chips de la memoria.
- Tarjeta de interfaz de red (NIC, Network Interface Card).
- Tarjeta de video o tarjeta gráfica.
- Tarjeta de sonido.
- Puerto paralelo.
- Puerto serie.
- Puerto del ratón.
- Puerto del teclado.
- Cable de alimentación.
- Puerto Bus serie universal (USB, Universal Serial Bus).

1.5.- COMPUTADORA DE ESCRITORIO FRENTE A COMPUTADORA PORTÁTIL.

Las computadoras portátiles se están haciendo cada vez más populares. La principal diferencia entre las computadoras de escritorio y las portátiles, aparte del hecho que los componentes portátiles son más pequeños que los de una PC, es que los portátiles ofrecen más movilidad y portabilidad de los PC de escritorio. Las ranuras de expansión son donde se conectan los dispositivos como NIC, módems, discos duros y otros dispositivos (normalmente del tamaño de una tarjeta de crédito).

Las ranuras de expansión se conocen como Asociación internacional de tarjetas de memoria de computadoras personales *(PCMCIA, Personal Computer Memory Card Internacional Association).*

1.6.- TARJETAS DE INTERFAZ DE RED.

Una NIC es una placa de circuito impreso que proporciona capacidades de comunicación de red hacia y desde una PC. También denominada adaptador de LAN, se conecta a la placa madre y proporciona un puerto para conectarse a la red. La NIC constituye la interfaz de la computadora con la LAN.

Una NIC se comunica con la red a través de un cable y con la computadora a través de una ruta de expansión. Cuando una NIC está instalada en una computadora,

requiere una solicitud de interrupción *(IRQ, Interrupt Requuest)* para un servicio desde el CPU, así como una dirección de entrada/salida (E/S), un espacio en memoria para el sistema operativo (como Linux o Windows) y controladores para llevar a cabo su función. La IRQ es una señal que informa al CPU de que ha ocurrido un evento del que necesita su atención. La IRQ se envía sobre una línea hardware al microprocesador. Un ejemplo de interrupción se da cuando se pulsa una tecla en el teclado. El CPU debe llevar el carácter del teclado a la RAM. Una dirección de (E/S) es una posición de memoria empleada para introducir o recuperar datos de una computadora mediante un dispositivo auxiliar.

Cuando elija una NIC para una red considere lo siguiente:

- Tipo de red.
- Tipo de medio.
- Tipo de Bus del sistema.

1.7.- INSTALACIÓN DE NIC Y MÓDEMS.

La conectividad a internet requiere una tarjeta adaptadora, que puede ser un módem o una NIC. Un módem es un dispositivo electrónico que se utiliza para las comunicaciones entre computadoras a través de la línea telefónica. Permite la transferencia de datos entre las computadoras sobre la red pública de teléfonos conmutada *(PSTN, Public Switched Telephone Netwok)*. Normalmente los módems envían datos en bloques de bits. Después de cada bloque, se ejecuta un cálculo matemático básico para analizar el bloque y a la computadora del extremo receptor se le pregunta si está de acuerdo con el resultado. Si aparece alguna diferencia, el bloque se envía de nuevo. Los módems convierten los datos digitales en señales analógicas para su transmisión sobre la PSTN y, después, convierten las señales analógicas de nuevo en bloques de datos en el extremo receptor.

El termino módem deriva de la función que realiza de este dispositivo. El proceso de convertir señales analógicas y viceversa se denomina modulación/desmodulación (de aquí el termino de módem). Los módems se pueden instalar internamente o conectar de forma externa a la computadora a través de una interfaz serie o USB. Los módems conectan la computadora a la red, marcando el número de teléfono de módem de otra computadora, normalmente el del proveedor de servicios de internet (ISP, *Internet Service Provider).*

1.8.- MODELO DE REFERENCIA OSI.

El primer desarrollo de las LAN, MAN y WAN fue en muchos sentidos caótico. A principios de los 80, esas empresas comenzaron a experimentar las secuelas del crecimiento en todas las expansiones que realizaron. Incluso fue más difícil para las redes que emplearon especificaciones e implementaciones diferentes para comunicarse entre sí. Comprendieron entonces que necesitaban adaptarse de los sistemas de red propietarios (patentados). Los sistemas patentados se desarrollan, poseen y controlan en privado. En la industria de las computadoras, patentado es lo opuesto a lo abierto. Patentado quiere decir que un grupo, o un pequeño grupo de empresas, controla toda la evolución y utilización de una tecnología. Abierto significa el libre uso de la tecnología disponible para el gran público.

Para solucionar el problema de la incompatibilidad e incapacidad de comunicación entre los diferentes sistemas de red, la Organización internacional de normalización (ISO, *Internacional Organization for Standardization*) investigó los esquemas de red, como de DECnet, SNA *(System Network Architecture*, arquitectura del sistema red*)* y TCP/IP, para encontrar un conjunto de normas. Como resultado de la investigación, la ISO creó un modelo de red que podía ayudar a los fabricantes a crear redes que fuesen compatibles que pudiesen operar con otras redes.

El proceso de dividir las comunicaciones complejas en tareas más pequeñas y sencillas, se podría compara con el proceso de construcción de un automóvil. Cuando se toma como un todo, el diseño, la fabricación y el ensamblaje de un automóvil es un proceso muy complejo. Es improbable que una persona sepa cómo realizar todas las tareas que se llevan a cabo para construir un automóvil desde el principio. Éste es el motivo por el que los ingenieros diseñan el coche, los técnicos de fabricación diseñan los moldes para crear las partes y los técnicos de ensamblaje unen cada parte del coche.

El modelo de referencia OSI, lanzado en 1984, fue el esquema descriptivo que creó la ISO. Este modelo proporcionó a los fabricantes un conjunto de normas que podrían facilitar una mayor compatibilidad e interoperabilidad entre los diferentes tipos de tecnologías de red producidos por muchas de las empresas de todo el mundo.

El modelo de referencia OSI es el modelo principal para las comunicaciones de red. Aunque existen otros modelos, la mayoría de los fabricantes actuales relacionan sus productos con el modelo de referencia OSI, especialmente cuando requieren educar a los usuarios en el empleo de sus productos.

Lo consideran la mejor herramienta disponible para enseñar cómo se envían y reciben los datos en la red.

El modelo de referencia OSI define las funciones de red que suceden en cada capa. Y lo más importante, este modelo es un armazón que se puede emplear para comprender como viaja la información a través de la red. Además, puede usarse para visualizar como la información, o paquetes de datos, viaja desde las aplicaciones (hojas de cálculo, documentos, etc.), por un medio de red (por ejemplo, los cables), hasta otras aplicaciones que están ubicadas en otra computadora de la red, aunque el emisor y receptor tengan diferentes tipos de red.

El modelo de referencia OSI tiene 7 capas numeradas, cada una ilustrando una función de red en particular.

- Capa 7: Capa de aplicación.
- Capa 6: Capa de presentación.
- Capa 5: Capa de sesión.
- Capa 4: Capa de transporte.
- Capa 3: Capa de red.
- Capa 2: Capa de enlace de datos.
- Capa 1: Capa física.

Esta separación de las funciones de la red se llama división en capas. Dividir la red en estas 7 capas proporciona las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Facilita la normalización de los componentes de la red, al permitir el desarrollo y el soporte de múltiples fabricantes.
- Permitir que diferentes tipos de hardware y software de red se comuniquen entre sí.
- Impide que los cambios en una capa afecten a las otras por lo que se pueden desarrollar más rápidamente.
- Divide la comunicación de la red en partes más pequeñas para ser más fácil su comprensión y entendimiento.

Al trabajar con las capas del modelo de referencia OSI, entenderá cómo viajan los paquetes de datos a través de una red y qué dispositivos operan en cada capa. Como resultado, entenderá cómo solucionar problemas en la red si se producen durante el flujo del paquete de datos.

1.8.1.- FUNCIONES Y CAPAS OSI.

El Modelo de Referencia de Interconexión de Sistemas Abiertos, OSI-RM (Open System Interconection-Reference Model) proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red utilizados por las empresas a nivel mundial.

Para poder simplificar el estudio y la implementación de la arquitectura necesaria, la ISO dividió el modelo de referencia OSI en capas, entendiéndose por capa una entidad que realiza de por sí una función específica.

Cada capa define los procedimientos y las reglas (protocolos normalizados) que los subsistemas de comunicaciones deben seguir, para poder comunicarse con sus procesos correspondientes de los otros sistemas. Esto permite que un proceso que se ejecuta en una computadora, pueda comunicarse con un proceso similar en otra computadora, si tienen implementados los mismos protocolos de comunicaciones de capas OSI.

1.8.2.- ESTRUCTURA DE NIVELES.

CAPA 7: LA CAPA DE APLICACIÓN. La capa de aplicación es la capa del modelo OSI más cercana al usuario, y está relacionada con las funciones de más alto nivel, proporcionando soporte a las aplicaciones o actividades del sistema, suministrando servicios de red a las aplicaciones del usuario y definiendo los protocolos usados por las aplicaciones individuales.

Es el medio por el cual los procesos las aplicaciones de usuario acceden a la comunicación por red mediante el entorno OSI, proporcionando los procedimientos precisos para ello.
Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo (procesadores de texto, hojas de cálculo, navegadores web, etc.).

La capa de aplicación establece la disponibilidad de los distintos elementos que deben participar en la comunicación, sincroniza las aplicaciones que cooperan entre sí y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.

CAPA 6: LA CAPA DE PRESENTACIÓN. La capa de presentación proporciona sus servicios a la capa de aplicación, garantizando que la información que envía la capa de aplicación de un sistema pueda ser entendida y utilizada por la capa de aplicación de otro, estableciendo el contexto sintáctico del diálogo.
Su función principal es aislar a las capas inferiores del formato de los datos de las aplicaciones específicas, transformando los formatos particulares (ASCII, EBCDIC, etc.) en un formato común de red, entendible por todos los sistemas y apto para ser enviado por red.
Es también las responsable de la obtención y de la liberalización de la conexión de sesión cuando existan varias alternativas disponibles.

Traducir entre varios formatos de datos utilizando un formato común, estableciendo la sintaxis y la semántica de la información transmitida.
Para ello convierte los datos desde el formato local al estándar de red y viceversa.

CAPA 5: LA CAPA DE SESIÓN. La capa de sesión proporciona sus servicios a la capa de presentación, proporcionando el medio necesario para que las entidades de presentación de dos host que se están comunicando por red organicen y sincronicen su diálogo y procedan al intercambio de datos.

CAPA 4: LA CAPA DE TRANSPORTE. La capa de transporte proporciona sus servicios a la capa de sesión, efectuando la transferencia de datos entre dos entidades de sesión.

Para ello, divide los datos originados en el host emisor en unidades apropiadas, denominadas segmentos, que vuelve a reensamblar en el sistema del host receptor.
La capa de transporte es la primera que se comunica directamente con su capa par de destino, ya que la comunicación de las capas anteriores es de tipo máquina a máquina.

La capa de transporte intenta suministrar un servicio de transporte de datos que aísle las capas superiores de los detalles del mismo, encargándose de conseguir una transferencia de datos segura y económica y un transporte confiable de datos entre los nodos de la red.

Para ello, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales, proporcionando un servicio confiable mediante el uso de sistemas de detección y recuperación de errores de transporte.
Controla la interacción entre procesos usuarios en las máquinas que se comunican. Incluir controles de integración entre usuarios de la red para prevenir perdidas o doble procesamiento de transmisiones.

CAPA 3: LA CAPA DE RED. La capa de red proporciona sus servicios a la capa de transporte, siendo una capa compleja que proporciona conectividad y selección de la

mejor ruta para la comunicación entre máquinas que pueden estar ubicadas en redes geográficamente distintas.

Es la responsable de las funciones de conmutación y enrutamiento de la información (direccionamiento lógico), proporcionando los procedimientos necesarios para el intercambio de datos entre el origen y el destino, por lo que es necesario que conozca la topología de la red (forma en que están interconectados los nodos), con objeto de determinar la ruta más adecuada.
En esta capa es donde trabajan los routers, dispositivos encargados de encaminar o dirigir los paquetes de datos desde el host origen hasta el host destino a través de la mejor ruta posible entre ellos.

CAPA2: LA CAPA DE ENLACE DE DATOS. La capa de enlace proporciona sus servicios a la capa de red, suministrando un tránsito de datos confiable a través de un enlace físico.

Se ocupa del direccionamiento físico, la topología de red, el acceso a la misma, la notificación de errores, la formación y entrega ordenada de datos y control de flujo.
Su principal misión es convertir el medio de transmisión en un medio libre de errores de cualquier tipo.

CAPA 1: LA CAPA FÍSICA. La misión principal de esta capa es transmitir bits por un canal de comunicación, de manera que cuanto envíe el emisor llegue sin alteración al receptor.
La capa física proporciona sus servicios a la capa de enlace de datos, definiendo las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales, relacionando la agrupación de circuitos físicos a través de los cuales los bits son transmitidos.

1.9.- TERMINOLOGÍA DE LAS REDES.

Esta sección introduce el concepto y la historia de las redes de datos. También explica las características básicas de los siguientes tipos de redes:

- Redes de área local (LAN, *Loca-Area Networks.)*
- Redes de área amplia (WAN, *Wide-Area Networks).*
- Redes de área metropolitana (MAN*, Metropolitan-Area Networks).*
- Redes de área de almacenamiento (SAN, *Storage-Area Networks).*
- Centros de datos.
- Intranet.
- Extranet.
- Redes privadas virtuales (VPN, *Virtual Private Network).*

1.10.- REDES DE DATOS.

IPX/SPX. Internet Packet eXchange/Sequenced Packet eXchange. Es el conjunto de protocolos de bajo nivel utilizados por el sistema operativo de red Netware de Novell. SPX actúa sobre IPX para asegurar la entrega de los datos.

DECnet. Es un protocolo de red propio de Digital Equipement Corporation (DEC), que se utiliza para las conexiones en red de los ordenadores y equipos de esta marca y sus compatibles.

Está muy extendido en el mundo académico.

Uno de sus componentes, LAT (Local Area Transport, transporte de área local), se utiliza para conectar periféricos por medio de la red y tiene una serie de características de gran utilidad como la asignación de nombres de servicio a periféricos o los servicios dedicados.

X.25. Es un protocolo utilizado principalmente en WAN y, sobre todo, en las redes públicas de transmisión de datos. Funciona por conmutación de paquetes, esto es, que los bloques de datos contienen información del origen y destino de los mismos para que la red los pueda entregar correctamente aunque cada uno circule por un camino diferente.

TCP/IP. Este no es un protocolo, si no un conjunto de protocolos, que toma su nombre de los dos más conocidos: TCP (Transmission Control Protocol, protocolo de control de transmisión) e IP (Internet Protocol). Esta familia de protocolos es la base de la red Internet, la mayor red de ordenadores del mundo. Por lo cual, se ha convertido en el más extendido.

APPLETALK. Este protocolo está incluido en el sistema operativo del ordenador Apple Macintosh desde su aparición y permite interconectar ordenadores y periféricos con gran sencillez para el usuario, ya que no requiere ningún tipo de configuración por su parte, el sistema operativo se encarga de todo. Existen tres formas básicas de este protocolo:

LOCALTALK. Es la forma original del protocolo. La comunicación se realiza por uno de los puertos serie del equipo. La velocidad de transmisión no es muy rápida pero es adecuada para los servicios que en principio se requerían de ella, principalmente compartir impresoras.

ETHERTALK. Es la versión de Appletalk sobre Ethernet. Esto aumenta la velocidad de transmisión y facilita aplicaciones como la transferencia de ficheros.

TOKENTALK. Es la versión de Appletalk para redes Tokenring.

NetBEUI. NetBIOS Extended User Interface (Interfaz de usuario extendido para NetBIOS). Es la versión de Microsoft del NetBIOS (Network Basic Input/Output System, sistema básico de entrada/salida de red), que es el sistema de enlazar el

software y el hardware de red en los PCs. Este protocolo es la base de la red de Microsoft Windows para Trabajo en Grupo.

REDES DE COBERTURA LOCAL (LAN). Una Red de Área Local (LAN) es un sistema por el cual se interconectan distintos equipos usando un solo medio de transmisión. Consiste en varias computadoras y periféricos cableados juntos en un área limitada, como el departamento de una compañía o un solo edificio.

Las redes locales se instalan para compartir recursos, impresoras o discos duros; para compartir información, tal es el caso de bases de datos; tener acceso a computadores centrales; tener comunicación más expedita usando el correo electrónico; y para tener conectividad, por ejemplo interconexión de diferentes equipos de distintos proveedores.
A una LAN se puede conectar computadoras personales, servidores de: comunicaciones, de faxes, de red; minicomputadoras, computadoras centrales (MainFrames) e incluso otras LAN.

Hay muchos beneficios en el uso de LAN, incluyendo ahorros al compartir datos y periféricos, estandarización de aplicaciones, adquisición de datos expedita y comunicaciones más eficientes entre el personal.

Hoy en día las redes se han expandido más allá de las LAN para cubrir el país y alrededor del mundo para formar las WAN (Wide Area Network).

1.11.- SEÑALIZACIÓN.

La información se coloca en el medio a través de uno de los métodos básicos de señalización: Baseband y Broadband.

En la señalización tipo baseband, la señal codificada es puesta directamente en el medio como una corriente continua de transiciones de voltaje sobre el medio físico como el cobre o como pulsos luminosos en una fibra óptica. En un momento dado sólo un nodo puede poner señales en el medio. Las señales en banda base deben ser repetidas periódicamente a lo largo de grandes distancias con el objeto de evitar pérdidas o interferencias debido a la degradación de la señal. La máxima distancia entre repetidores es una función de las propiedades del medio de transmisión, del uso de conectores intermedios y de la velocidad misma de transmisión. Por lo general, al aumentar la velocidad se reduce esta distancia.

En la señalización tipo broadband, o de banda ancha, se utilizan señales analógicas y técnicas de multiplexaje sobre el medio de transmisión para permitir que más de un nodo transmita a la vez. Se pueden crear múltiples bandas de frecuencia (canales) mediante FDM. Un sistema típico de broadband tiene B=300 Mhz, se pueden dividir en canales de 6 Mhz teniendo pares de canales designados para comunicación bidireccional. Un canal estándar de 6 Mhz puede trabajar a velocidades de hasta 5 Mbps, dos canales adyacentes de 6 Mhz pueden ser utilizados para proporcionar un canal sencillo de 12 Mhz con velocidades de hasta 10 Mbps. La operación de broadband requiere que la función de modulación y demodulación sean hechas en los nodos de origen y destino respectivamente resultando un incremento en el costo

por nodo sobre los sistemas de banda base, sin embargo esto permite que las señales broadband alcancen distancias más grandes entre repetidores.

1.12.- TOPOLOGIAS.

Una topología de red define como están conectadas las computadoras, impresoras, dispositivos de red y otros dispositivos. En otras palabras, una topología de red describe la disposición de los cables y los dispositivos, así como las rutas utilizadas para las transmisiones de datos. La topología influye enormemente en el funcionamiento de la red.

Las redes pueden tener una topología física y una topología lógica. La topología física se refiere a la disposición física de los dispositivos y los medios. Las topologías físicas más comunes son las siguientes:

- Bus
- Anillo
- Estrella
- Estrella extendida
- Jerárquica
- Malla

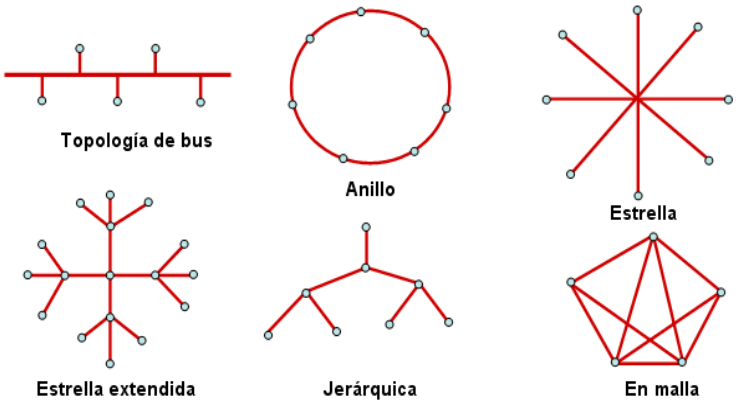


Fig.1.-Topologías físicas.

TOPOLOGÍA DE BUS. Comúnmente conocida como bus línea, una topología de bus conecta todos los dispositivos utilizando un solo cable. Este cable va de una computadora a la siguiente, al igual que un autobús de línea va de una ciudad a otra.

Con una topología en bus física, el segmento de cable principal debe finalizar con un terminador que absorba la señal cuando ésta alcanza el final de la línea o cable. Si no hay un terminador, la señal eléctrica que representa los datos rebotará al otro extremo del cable, provocando errores en la red.

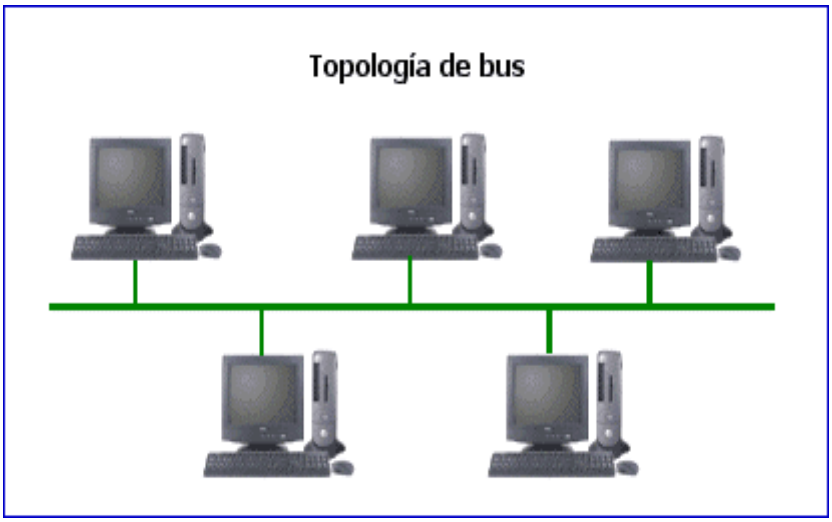


Fig.2.- Topología de bus.

TOPOLOGÍA DE ESTRELLA Y ESTRELLA EXTENDIDA. La topología en estrella es la topología más frecuente en las LAN Ethernet. Una vez instalada, la topología en estrella se parece a los rayos de una rueda de bicicleta. La topología en estrella está constituida por un punto de conexión central que es un dispositivo (como un hub, un switch o un router) donde se encuentran todos los segmentos de cable. Cada uno de los hosts de la red está conectado al dispositivo central con su propio cable.

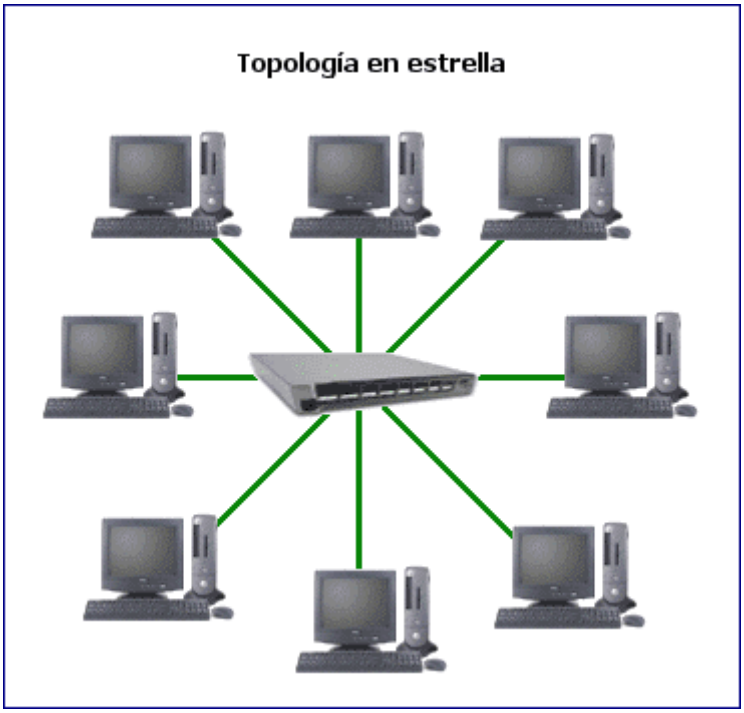


Fig.3.- Topología de estrella.

Aunque la implementación de una topología en estrella física es más costosa que la de la topología en bus física, sus ventajas contrarrestan ese coste adicional. Como cada host está conectado al dispositivo central con su propio cable, cuando este cable tiene un problema, sólo ese host se ve afectado; el resto de la red permanece operativa. Esta ventaja es extremadamente importante y debido a ella casi todas las nuevas LAN Ethernet que se diseñan una topología en estrella física.

Un punto de conexión central podría ser deseable para la seguridad o el acceso restringido, pero esto también es un importante inconveniente de la topología en estrella. Si falla el dispositivo central, la red entera se desconecta.

Cuando una red en estrella se expande para incluir un dispositivo de red adicional conectado al dispositivo de red principal, se conoce como topología en estrella extendida.

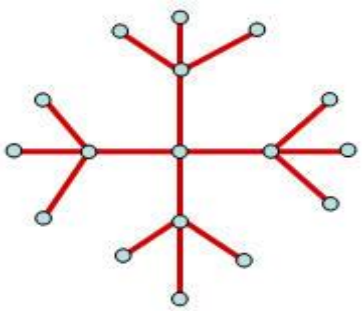


Fig.4.- Topología de estrella extendida.

TOPOLOGÍA EN ANILLO. La topología en anillo lógica es otra topología importante en la conectividad LAN. Como su nombre indica, los hosts están conectados en forma de anillo o circulo. A diferencia de la topología en bus física, la topología en anillo no tiene principio o fin que deba terminarse. Los datos se transmiten en un sentido, al contrario que en la topología en bus lógica. Una trama viaja alrededor del anillo, parando en todos los nodos, Si un nodo quiere transmitir los datos, tiene permiso de añadir esos datos, así como la dirección de destino, a la trama. Ésta continúa entonces viajando por e anillo hasta encontrar el nodo de destino, que extrae los datos de la trama, La ventaja de utilizar este tipo de método es que no hay colisiones de los paquetes de datos.

Hay dos tipos de anillos:

- Anillo simple.
- Anillo doble.

En un anillo simple, todos los dispositivos de la red comparten un solo cable y los datos viajan en una única dirección. Cada dispositivo espera su turno para enviar datos por la red. La mayoría de las topologías de anillo simple están cableadas realmente por una estrella.

Fig.5.-Topología de anillo.

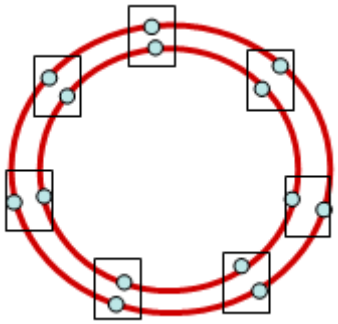


Fig.6.-Topología doble de anillo.

En un anillo doble, dos anillos permiten que los datos se envíen en ambas direcciones. Esta configuración crea redundancia (tolerancia a fallos), lo que significa que uno de los anillos falla, los datos pueden transmitirse por el otro. Además, si ambos anillos fallan, una “reiniciación” en el fallo puede devolver la topología a un anillo.

TOPOLOGÍA JERÁRQUICA. Una topología jerárquica es similar a una topología en estrella extendida. La principal diferencia es que no utiliza un nodo central. En su lugar, utiliza un nodo troncal del que parten ramas a otros nodos. Existen dos tipos de topologías en árbol binario (cada nodo se divide en dos enlaces) y el árbol backbone (un tronco backbone tiene nodos rama con enlaces de él).

TOPOLOGÍAS EN MALLA COMPLETA Y EN MALLA PARCIAL. La topología en malla completa conecta todos los dispositivos (nodos) con todos los demás para conseguir redundancia y tolerancia a fallos. El cableado en una topología en malla completa tiene diferentes ventajas e inconvenientes. La ventaja es que cada nodo está conectado físicamente con todos los demás, creándose una.

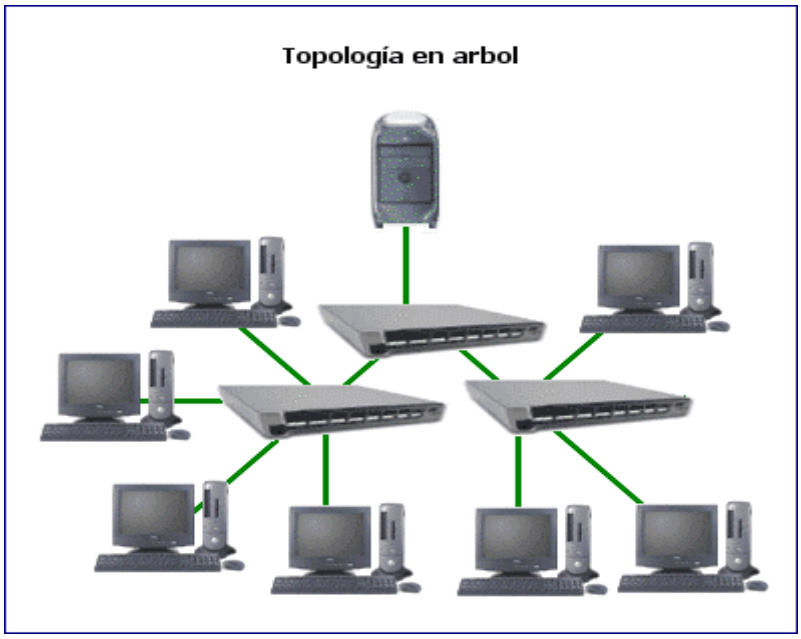


Fig.7.- Topología en árbol.

Conexión redundante. Si falla cualquiera de los enlaces, la información puede fluir por otros muchos enlaces para alcanzar su destino. El principal inconveniente es que para algo más que un pequeño número de nodos, la cantidad de medios para los enlaces y el número de conexiones en las líneas puede ser abrumador. La implementación de una topología en malla completa es costosa y compleja. Normalmente se implementa en WAN entre routers.

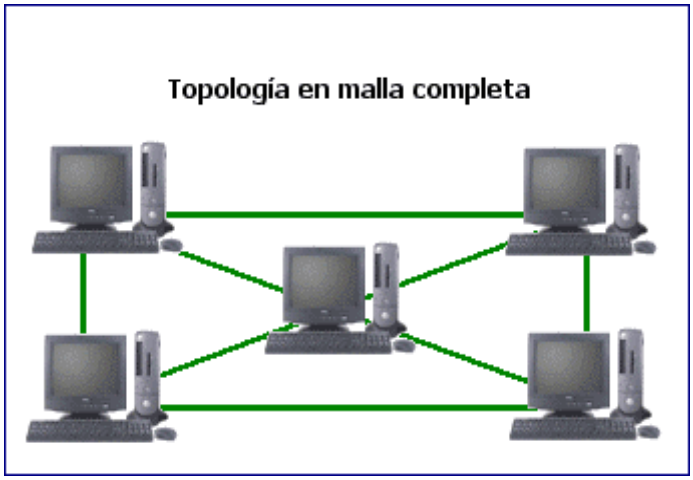


Fig.8.- Topología en malla completa.

En una topología en malla principal, al menos uno de los dispositivos mantiene múltiples conexiones con otros sin estar mallado por completo. Una topología en malla parcial todavía proporciona redundancia al conectar con varias rutas alternativas. Si una ruta no se puede utilizar, los datos toman otra diferente, aunque sea más larga. La topología en malla parcial se utiliza en muchos backbones de telecomunicaciones, así como en Internet.

TOPOLOGÍA LÓGICA. Una topología lógica de red se refiere a cómo los hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son difusión y transmisión de testigos.

La topología de difusión simplemente significa que cada host dirige sus datos a una NIC en particular, a una dirección multidifusión o una dirección de difusión en el medio de red. No hay un orden que las estaciones deban seguir para utilizar la red. El primero que llega es el primero que sirve. Ethernet también funciona de este modo.

La segunda topología lógica es la transmisión de testigos, que controla el acceso a la red pasando un testigo electrónico secuencialmente a cada host. Cundo un host recibe el testigo, puede enviar datos por la red. Si el host no tiene datos que enviar, pasa el testigo al siguiente host, y el proceso se vuelve a repetir, Token Ring y FDDI son dos ejemplos de redes que utilizan la transmisión de testigos, y ambas son ejemplos de transmisión de testigos en una topología en anillo física.

1.13.- ENRUTAMIENTO Y PROTOCOLOS.

DIRECCIONAMIENTO DE RED Y DE HOST. El router utiliza la dirección de red para identificar la red de destino de un paquete dentro de un internetworking de redes. Muestra tres números de red que identifican los segmentos conectados al router.

Red	Host
1	1 2 3
2	1
3	1

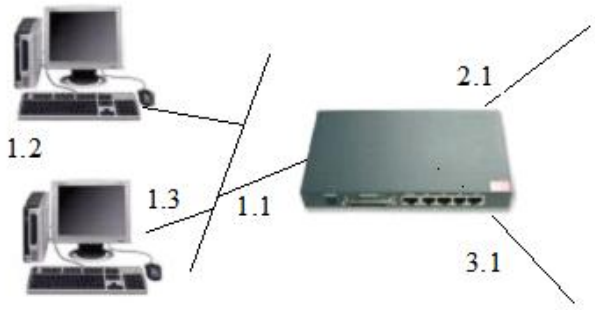


Fig.9.-Direcciones de red con partes de host.

La mayoría de los esquemas de protocolo de direccionamiento de red usan alguna forma de dirección de nodo o host. En algunos protocolos de la capa de red, un administrador asigna las direcciones de host de red siguiendo un plan de direccionamiento de internetwork predeterminado. En otros protocolos, la asignación de direcciones de host es parcial o completamente dinámica. En la figura anterior, tres host comparten el número de red.

SELECCIÓN DE UNA RUTA Y CONMUTACIÓN DE PAQUETES. Generalmente, un router transmite un paquete desde un enlace de datos a otro usando dos funciones básicas.

- Una función de determinación de ruta
- Una función de conmutación

La figura que a continuación se muestra es la forma en que los routers usan el direccionamiento para las funciones de enrutamiento y conmutación. El router utiliza la parte de red de la dirección para seleccionar la ruta y pasar el paquete al siguiente router de la misma.

La función de conmutación permite al router aceptar un paquete de una interfaz y reenviarlo a otra, mientras que la función de determinación de la ruta le permite seleccionar la interfaz más adecuada para el reenvío de dicho paquete. El router final (el que está conectado a la red de destino) utiliza la parte de nodo de la dirección para entregar el paquete al host correcto.

Red de Destino	Dirección y Puerto de router
1.0 2.0 3.0	1.1 2.1 3.1

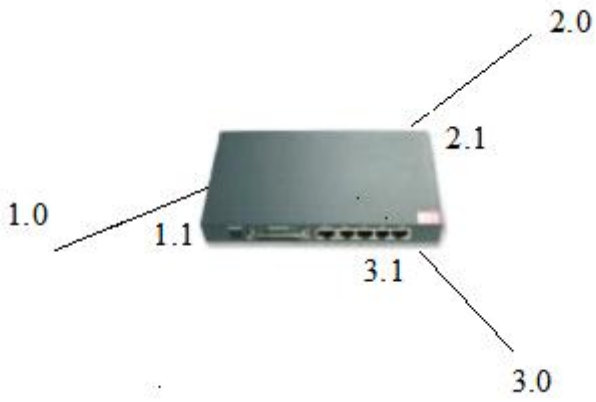


Fig.10.-Forma en que los routers usan el direccionamiento para las funciones de enrutamiento y conmutación.

1.14.- PROTOCOLOS ENRUTADOS FRENTE A PROTOCOLOS DE ENRUTAMIENTO.

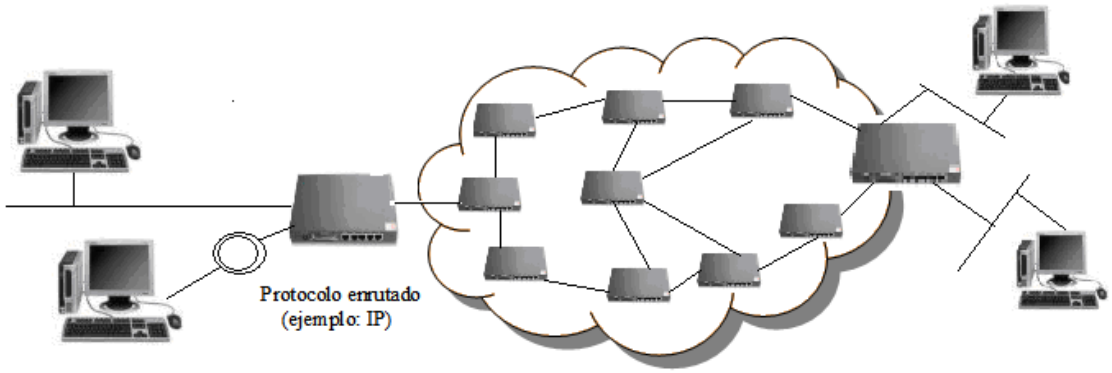
Debido a lo parecido en ambos términos, suelen producirse confusiones acerca del protocolo enrutado y el protocolo de enrutamiento. Lo que sigue a continuación puede ayudar a clarificar algo los conceptos.

- Protocolo enrutado. Es cualquier protocolo de red que ofrezca suficiente información en su dirección de capa de red como para permitir que un paquete sea enviado desde un host a otro en base al esquema de direccionamiento. Los protocolos enrutados definen el formato de los campos dentro de un paquete. Generalmente, los paquetes suelen ser transportados entre sistemas finales.

Un protocolo enrutado utiliza la tabla de enrutamiento para enviar paquetes. IP (Protocolo Internet, Internet Protocol) es un buen ejemplo de protocolo enrutado.

- Protocolo de enrutamiento. Es cualquier que soporte un protocolo enrutado y que suministre los mecanismos necesarios para compartir la información de enrutamiento. Los mensajes de un protocolo de enrutamiento se mueven entre los routers. Un protocolo de enrutamiento permite a los routers comunicarse con otros routers para actualizar y mantener las tablas. A continuación se muestran diversos protocolos de enrutamiento TCP/IP:

    - RIP (Protocolo de información de enrutamiento, Routing Information Protocol).
    - IGRP (Protocolo de enrutamiento de gateway interior, Interior Gateway Routing Protocol).
    - EIGRP (Protocolo de enrutamiento de gateway interior mejorado, Enhanced Interior Gateway Routing Protocol).
    - OSPF (Primero la ruta libre más corta, Open Shortest Path First).



Protocolo de Red	Red de Red	Puerto de Salida a utilizar
Protocolo	1.0 2.0 3.0	1.1 2.1 3.1

Fig.11.- Protocolo enrutado de IP.

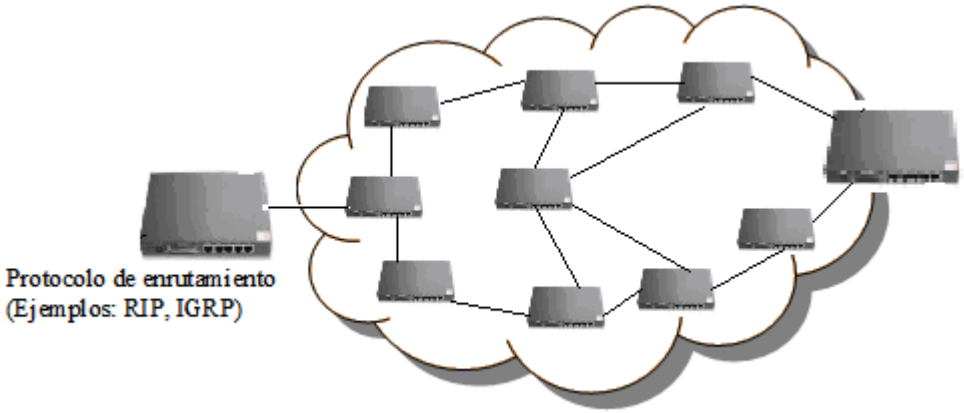


Fig.12.-Protocolos de router de enrutamiento

1.15.- FUNCIONAMIENTO DEL PROTOCOLO DE LA CAPA DE RED.

Suponga que una aplicación host tiene que enviar un paquete a una red diferente. El host direcciona la trama del enlace de datos al router usando la dirección de una de las interfaces del router. La capa de red del router examina la cabecera de capa 3 del paquete entrante para determinar la red de destino y poder referenciar después la tabla de enrutamiento, la cual asocia las redes con las interfaces salientes.

El paquete se encapsula de nuevo en la trama de enlace de datos adecuada a la interfaz seleccionada y se pone en cola para su distribución al siguiente salto en la ruta.

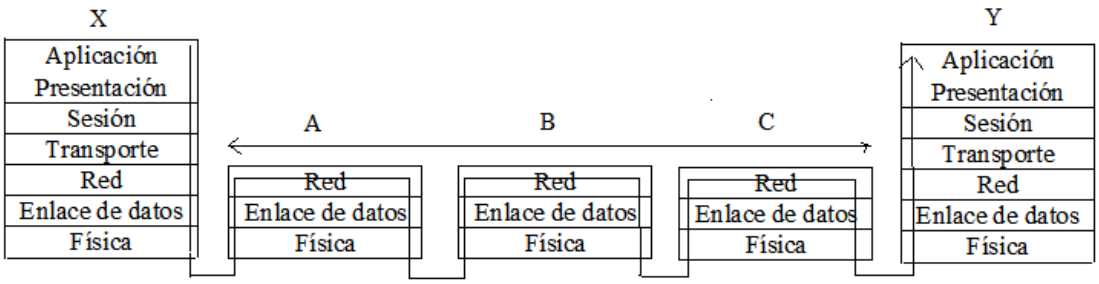


Fig.13.-Servicios de router

Este protocolo se realiza cada vez que el paquete se envía de un router a otro. Cuando dicho paquete alcanza el router conectado a la red del host de destino, se encapsula en el tipo de trama del enlace de datos de la LAN y se envía en dicho host.

1.16.- ENRUTAMIENTO MULTIPROTOCOLO.

Los routers son capaces de soportar múltiples protocolos de enrutamiento independientes y de mantener las tablas de enrutamineto de diversos protocolos enrutados. Esta capacidad les permite entregar paquetes de diferentes protocolos enrutados a través de los mismos enlaces de datos.

ENRUTAMIENTO ESTÁTICO. El enrutamiento no es nada más que direcciones para llegar de una red a otra. Estas direcciones, también conocidas como rutas, puede ser facilitadas a un router dinámicamente por otro router, aun que también pueden asignarse estáticamente por parte de un administrador. Esta sección se centra en las rutas asignadas por un administrador.

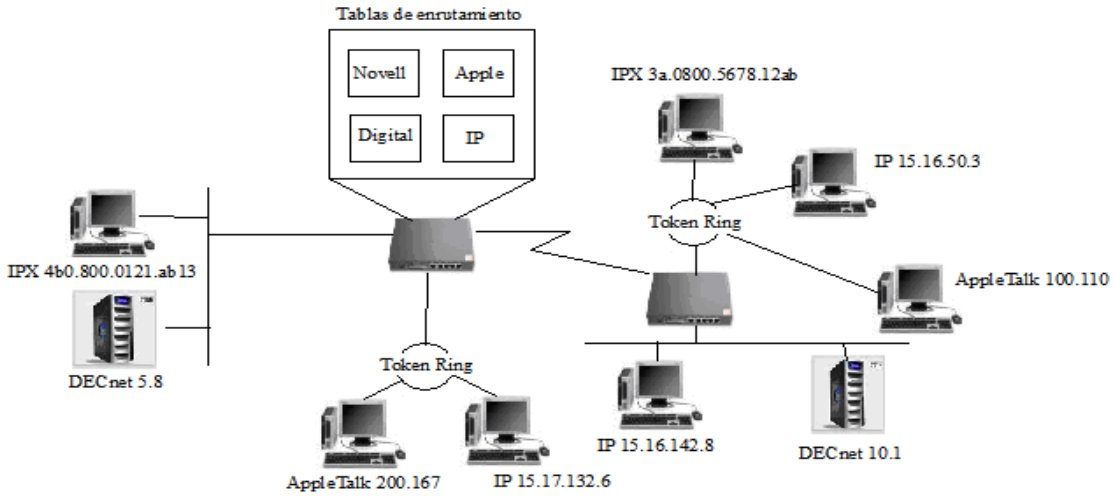


Fig.14.-Tráfico de un router.

RUTAS ESTÁTICAS CONTRA RUTAS DINAMICAS. La configuración de una ruta estática es una tarea manual llevada a cabo por un administrador d3e redes, el cual la introduce en la configuración de un router. Dicho administrador debe actualizar también la ruta siempre que una modificación en la topología de la internetwork obligue a dicha actualización.

La configuración de una ruta dinámica funciona de forma algo diferente. Después de que un administrador de redes ha introducido los comandos de configuración para iniciar un enrutamiento dinámico, un proceso de enrutamiento lleva acabo la actualización de la ruta siempre que se recibe nueva información desde la internetworking de redes. Estos cambios dinámicos son comunicados a otros routers como parte del proceso de actualización.

PROPÓSITO DE UNA RUTA ESTÁTICA. El enrutamiento estático tiene diversas aplicaciones útiles. El enrutamiento dinámico tiene a revelar toda la información posible acerca de un internetworking de redes, sin embargo, puede que por motivos de seguridad necesite que parte de dicho espacio permanezca oculto. El enrutamiento estático le permite indicar la información a revelar en redes restringidas. Cuando una red es accesible por una sola vía, puede ser suficiente una ruta estática a la red. Este tipo de red recibe el nombre de red de conexión única. Una red de conexión única es un área OSPF que dispone de una ruta predeterminada, rutas-áreas y rutas inter-áreas, pero no de rutas externas. El enrutamiento estático de una de estas redes evita la sobrecarga del enrutamiento dinámico.

CAPITULO 2 VPN.

2.1.- ¿QUÉ ES UNA VPN?

Una VPN es: usar accesos a una WAN pública (típicamente Internet), para conectar oficinas y usuarios remotos sin la necesidad de los costosos enlaces dedicados de las WAN públicas tradicionales.
Deberá de proveernos de algún método de encripción para los datos a ser transmitidos ya que estaremos enviando información privada por un canal público.
Los principales proveedores de accesos a Internet en México son: Telmex, Avantel, AT&T y Protel.
Consiste en aprovechar una infraestructura pública para simular una red privada. Para ello utilizan el encapsulamiento IP-IP, el direccionamiento es independiente del de la red pública, solución muy útil actualmente para comunicar una empresa a través de Internet, a menudo llevan un requerimiento de seguridad (encriptación con IPSec), se basa en la creación de túneles. Los túneles pueden conectar usuarios u oficinas remotas.

2.2.- VENTAJAS DE UNA VPN.

Las VPN son una salida al costo que puede significar el pagar una conexión de alto costo, para usar líneas alquiladas que estén conectadas a otros puntos que puedan hacer uso de la conexión a Internet o para hacer negocios con clientes frecuentes a través de la red.
Los datos son codificados o cifrados y recién enviados a través de la conexión, para de esa manera asegurar la información y el password que se esté enviando.
Esta tecnología proporciona un medio para aprovechar un canal público de Internet como un canal privado o propio para comunicar datos que son privados. Más aún, con un método de codificación y encapsulamiento, una VPN básica, crea un camino privado a través de Internet. Esto reduce el trabajo y riesgo en una gestión de red.
La tecnología de túneles está basada en estándares. Esta tecnología permite transmitir datos entre dos redes similares. A esto también se le llama "encapsulamiento", es decir, a la tecnología que coloca algún tipo de paquetes dentro de otro protocolo (TCP). Aparte de todo esto, también se añade otra información necesaria para poder descifrar la información que se encuentra codificada. Estos paquetes llegan a su destino después de haber atravesado Internet, pero para verificar que ha llegado al destino correcto se realiza un proceso de autentificación.
Las VPNs son una gran solución a distintos problemas, pero solo en el campo de la economía de los usuarios, porque por ejemplo, en el caso de que se realice una conexión entre dos sedes de empresas, una en Japón y la otra en Perú, sería muy costoso el realizar un cableado entre estos dos países, y un enlace inalámbrico satelital sería muy costoso. Es por ello que una red privada virtual es más económica porque solo se hace uso de Internet que es un conjunto de redes conectadas entre sí.

Las ventajas más significativas son:

a) El ahorro del coste de un enlace dedicado, uso de Internet para conectar centros de trabajo. En la siguiente imagen se muestra una comparación entre una línea dedicada y una VPN

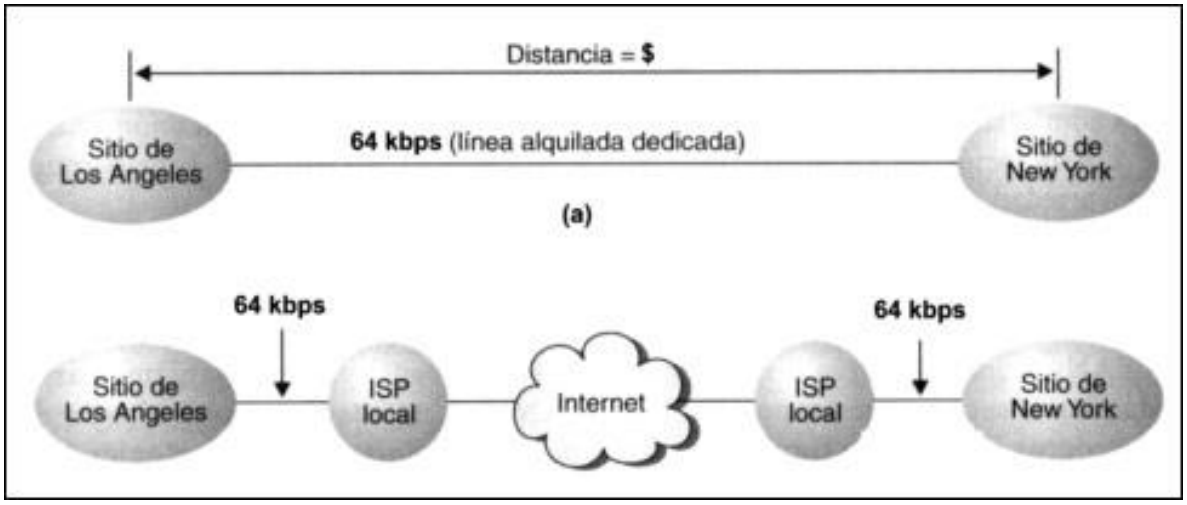


Fig.- 15 Línea dedicada V.S VPN

b) Escalabilidad: Las VPNs son arquitecturas de red más escalables y flexibles que las WAN tradicionales, debido a que permiten a las corporaciones agregar o eliminar sus sistemas localizados remotamente, “teletrabajadores” o aliados comerciales de forma fácil y poco costosa en función de las necesidades del negocio.

c) Seguridad: Bajo el esquema de VPN la conexión a través de Internet es cifrada. El servidor de acceso remoto exige el uso de protocolos de autenticación y cifrado. Los datos confidenciales quedan ocultos a los usuarios de Internet.

d) Compatibilidad: Como se aceptan la mayor parte de los protocolos de red más comunes (incluidos TCP/IP, IPX y NetBEUI).

2.3.- MEDIOS PARA VPN.

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación:

- Autenticación y autorización: ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.
- Integridad: La garantía de que los datos enviados no han sido alterados.
- Confidencialidad: Dado que los datos viajan a través de un medio potencialmente hostil como Internet, los mismos son susceptibles de intercepción, por lo que es fundamental el cifrado de los mismos. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma. Sé hace uso de algoritmos de cifrado
- No repudio: es decir, un mensaje tiene que ir firmado, y el que lo firma no puede negar que el mensaje lo envió él.

2.4.- INFRAESTRUCTURA REQUERIDA PARA UNA VPN.

- Acceso a Internet (Inalámbrico, ISDN, ADSL, etc.), Nuestros centros de trabajo deben de contar con acceso a Internet, se recomienda tener accesos de por lo menos de 128Kbps, cabe mencionar que en México la tecnología con mayor penetración en el país es el ADSL.
- Hardware/Software para servidor/cliente VPN

2.5.- TIPOS DE VPN.

Básicamente existen tres arquitecturas de conexión VPN:

VPN de acceso remoto.

Es quizás el modelo más usado actualmente y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autentificados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

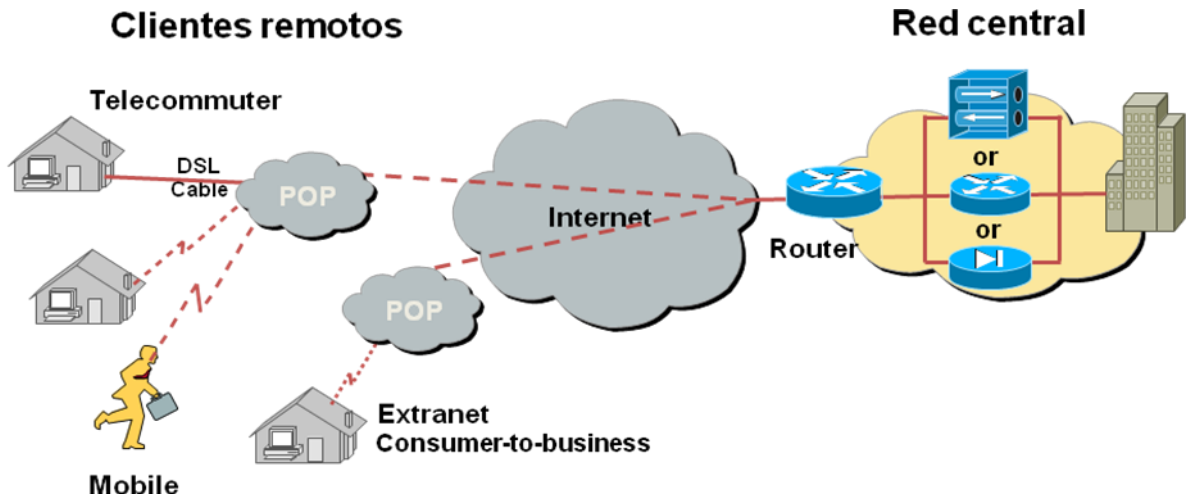


Fig.- 16 Arquitectura de VPN

VPN punto a punto.

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicional, sobre todo en las comunicaciones internacionales. Es más común el punto anterior, también llamada tecnología de túnel o tunneling.

Tunneling.- Internet se construyó desde un principio como un medio inseguro. Muchos de los protocolos utilizados hoy en día para transferir datos de una máquina a otra a través de la red carecen de algún tipo de cifrado o medio de seguridad que evite que nuestras comunicaciones puedan ser interceptadas y espiadas. HTTP, FTP, POP3 y otros muchos protocolos ampliamente usados, utilizan comunicaciones que viajan en claro a través de la red. Esto supone un grave problema, en todas aquellas situaciones en las que queremos transferir entre máquinas información sensible, como pueda ser una cuenta de usuario (nombre de usuario y contraseña), y no tengamos un control absoluto sobre la red, a fin de evitar que alguien pueda interceptar nuestra comunicación por medio de la técnica del hombre en el medio (man in the middle), como es el caso de la Red de redes.

El problema de los protocolos que envían sus datos en claro, es decir, sin cifrarlos, es que cualquier persona que tenga acceso físico a la red en la que se sitúan las máquinas puede ver dichos datos. De este modo, alguien que conecte su máquina a una red y utilice un sniffer recibirá y podrá analizar por tanto todos los paquetes que circulen por dicha red. Si alguno de esos paquetes pertenece a un protocolo que envía sus comunicaciones en claro, y contiene información sensible, dicha información se verá comprometida.

Si por el contrario, se cifran las comunicaciones con un sistema que permita entenderse sólo a las dos máquinas que son partícipes de la comunicación, cualquiera que intercepte desde una tercera máquina los paquetes, no podrá hacer nada con ellos, al no poder descifrar los datos. Una forma de evitar este problema, sin dejar por ello de utilizar todos aquellos protocolos que carezcan de medios de cifrado, es usar una técnica llamada tunneling.

Básicamente, esta técnica consiste en abrir conexiones entre dos máquinas por medio de un protocolo seguro, como puede ser SSH (Secure SHell), a través de las cuales realizaremos las transferencias inseguras, que pasarán de este modo a ser seguras. De esta analogía viene el nombre de la técnica, siendo la conexión segura (en este caso de ssh) el túnel por el cual se envían los datos para que nadie más aparte de los interlocutores que se sitúan a cada extremo del túnel, pueda ver dichos datos. Este tipo de técnica requiere de forma imprescindible tener una cuenta de acceso seguro en la máquina con la que se quiere comunicar.

VPN interna WLAN.

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

CAPITULO 3 IPSEC.

3.1 IPSEC SEGURIDAD EN INTERNET.

RFC-1636 describe la seguridad en la arquitectura de Internet, donde se informa sobre los requisitos para hacer segura la infraestructura de Internet, para evitar la monitorización no autorizada.
Con ello, se ha desarrollado IPSEC ofreciendo:
-conectividad segura con redes privadas virtuales (VPN), a través de túneles, que permitan el acceso remoto a través de Internet o acceso telefónico
-asegura la autentificación

3.2 INTRODUCCIÓN.

- Es una ampliación de IP, diseñada para funcionar de modo transparente en redes existentes
- Usa criptografía para ocultar datos
- Independiente de los algoritmos de cifrado
- Aplicable en IPv4 y obligatorio en IPv6
- Está formado por:
- Una Arquitectura (RFC 2401)
- Un conjunto de protocolos
- Una serie de mecanismos de autenticación y encriptado (DES, 3DES y mejor por hardware)
- Se especifica en los RFCs 1826, 1827, 2401, 2402, 2406 y 2408
- Integración de voz sobre VPN's (VoIP)

3.3 PRINCIPALES FUNCIONALIDADES DE IPSEC.

- AH (Autentication Header, RFC 2402): garantiza que el datagrama fue enviado por el remitente y que no ha sido alterado durante su viaje. Por ejemplo utilizando algoritmo MAC
- ESP (Encapsulating Security Payload, RFC 2406): garantiza que el contenido no pueda ser examinado por terceros (o que si lo es no pueda ser interpretado). Opcionalmente puede incluir la función de AH de autentificación.
- Ambos AH y ESP, definen una cabecera IPsec incluida en el paquete a enviar.
- ISAKMP (Internet Security Association and Key Management Protocol, RFC 2408): es un entorno que permite un mecanismo seguro (manual y automático) de intercambio de formatos de paquete y claves utilizadas en las tareas de encriptado y autentificación de AH y ESP. Incluye a IKE (Internet Key Exchange). Utiliza Diffie-Hellman y HMAC.

- SA (Security Association): conjunto de políticas y claves para establecer y proteger una conexión.

Encripción de IPsec.

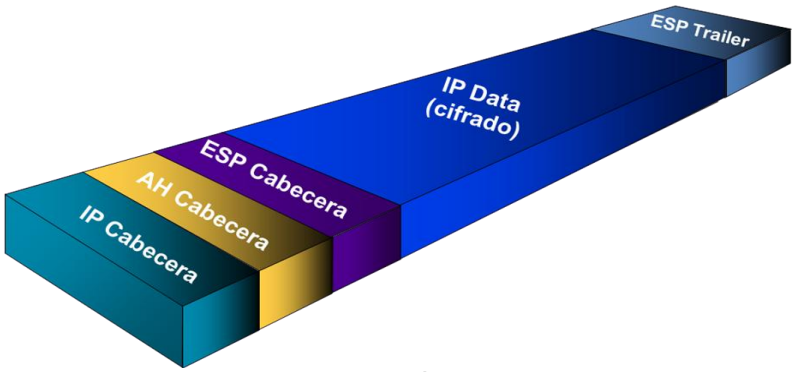


Fig.- 16 Encripción de IPSEC

3.4 MODOS DE FUNCIONAMIENTO.

- Modo transporte: comunicación segura extremo a extremo. Requiere implementación de IPSec en ambos hosts. No se cifra la cabecera IP.
- Modo túnel: comunicación segura entre routers únicamente, que ejecutan pasarelas de seguridad. Permite incorporar IPSec sin tener que modificar los hosts. A los paquetes se añade otra cabecera. Se integra cómodamente con VPNs

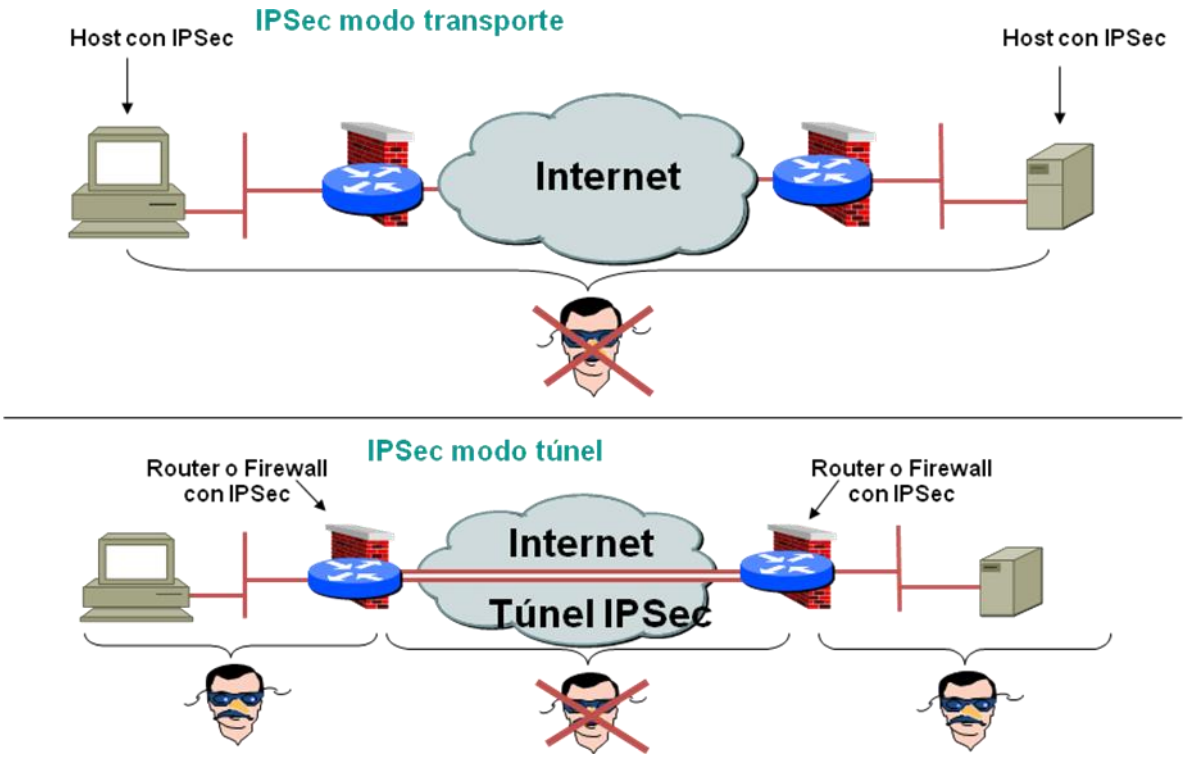


Fig. 17 Modos de IPSEC

CAPITULO 4 OPCIONES PARA TRANSPORTAR VOZ.

4.1.- VOIP.

VoIP significa Voz Sobre IP (Servicio de voz bajo protocolo de Internet), toma las señales de audio análogas, como las que escucha al hablar por teléfono, y las convierte en datos digitales que se pueden transmitir por Internet Si bien la idea de una red única, que permita la convergencia entre las redes de voz y datos no es nueva, la continua actualización y mejora de los sistemas de transmisión de datos, han hecho posible que un estándar (H.323) definido hace ya algún tiempo, esté empezando a dar sus primeros pasos significativos a otros estándar como SIP, IAX.

4.2.- H.323.

H.323 es una especificación de la ITU-T para transmitir audio, video y datos a través de una red de Protocolo Internet (IP), incluida la propia Internet. Cuando son compatibles con H.323, los productos y aplicaciones de los fabricantes pueden comunicarse e ínteroperar unos con otros. El H.323 estándar dirige la señalización y control de llamadas, transporte y control multimedia y control de ancho de banda para conferencias punto a punto y multipunto. La serie H de las recomendaciones también especifica H.320 para la Red Digital de Servicios Integrados (RDSI) y H3.24 para el servicio telefónico analógico convencional (POTS, plan old telephone service) como mecanismos de transporte.

El H323 estándar consta de los siguientes componentes y protocolos:

FUNCIÓN	PROTOCOLO
Señalización de llamadas	H.225
Control de medios	H.245
Còdecs de audio	G.711, G.722, G.723, G.728, G.729
Còdecs de video	H.261, H.263
Compartir datos	T.120
TRANSPORTE DE MEDIOS	RTP/RTCP

H.323 se creó originalmente para proveer de un mecanismo para el transporte de aplicaciones multimedia en LANs (Redes de área local) pero ha evolucionado rápidamente para dirigir las crecientes necesidades de las redes de VoIP.

¿Que son las Líneas IP Enlaces?. Son líneas telefónicas que permiten hacer llamadas locales, nacionales e internacionales a teléfonos fijos y celulares por una tarifa plana al mes.

Esto permite tener ahorros de hasta un 80% en el pago de su recibo telefónico, las Líneas IP de Enlaces conectan los servicios telefónicos tradicionales a través de Internet, permitiendo grandes ahorros.

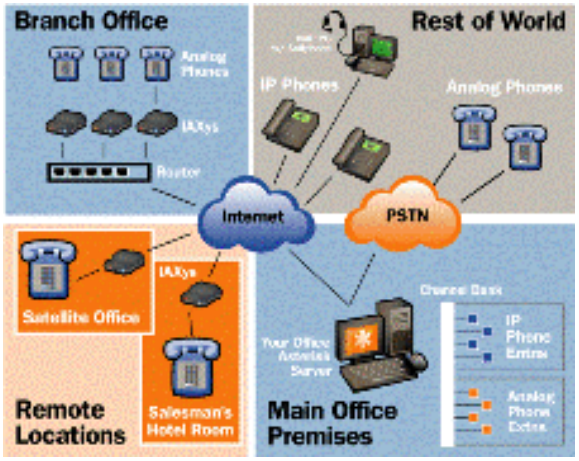


Fig.19.- Aplicación VoIP

4.3.- ARQUITECTURA DE RED.

El sistema H.323 se explica en las tres siguientes secciones:

- Elementos H.323.
- Conjunto de protocolo H.323.
- Flujos de llamadas H.323

4.4.- ELEMENTOS H.323

Los elementos de un sistema H.323 estos elementos incluyen terminales, gateways, gatekeepers y unidades de control multipunto (MCU, Multipoint Control Units).
Los terminales, a los que a menudo hace referencia como puntos finales, proporcionan conferencias punto a punto y multipunto para audio y de manera opcional, video y datos. Los gateways interconectan con la red pública de telefonía conmutada (PSTN) o la red ISDN (RDSI) para interworking el punto final de H.323. los gatekeepers proporcionan el control de admisión y servicio de traducción de direcciones para terminales o gateways. Las MCU son dispositivos que permiten que dos o más terminales o gateways realicen conferencias con sesiones de audio y/o video.

4.5.- TRANSPORTE DE MEDIOS (RTP/RTCP)

RTP proporciona transporte de medios en H.323. De manera mas especifica, RTP permite la entrega de extremo a extremo en tiempo real de audio, video y datos interactivos sobre las redes de unidifusión o multidifusión. Los servicios de empaquetamiento y transmisión incluyen la identificación de carga útil, la secuenciación, la marca de temporización y la monitorización.
RTP depende de otros mecanismos y de las capas bajas para asegurar la entrega a tiempo, la reserva de recursos, la fiabilidad y la QoS. RTCP monitoriza la entrega de datos y controla e identifica los servicios. El canal de medios se crea utilizando UDP, donde los flujos RTP actúan en un numero de puerto par y el flujo RTCP correspondiente actual en el siguiente numero de puertos mas alto (impar).

TERMINAL. Los terminales H.323 deben tener una unidad de control de sistema, una transmisión de medios, còdecs de audio e interfaz de red basada en paquetes. Los requisitos opcionales incluyen un codec de video y aplicaciones de datos de usuario.

Las siguientes funciones y posibilidades se encuentran dentro del ámbito del Terminal H.323:

- Unidad de control de sistema. Proporciona al H.225 y H.245 el control de llamadas, intercambio de capacidad, mensajería y señalización de comando para una actividad apropiada del Terminal.
- En las redes H.323, los procedimientos de control de llamadas se basan en la recomendación H.225 de la ITU-T, que especifica la utilización y el soporte de los mensajes de señalización Q.931. un canal de control de llamadas seguro se crea en una red IP en el puerto 1720 del TCP. Este puerto inicializa los mensajes de control de llamadas Q.931 entre dos puntos finales para los propósitos de conectar, mantener y desconectar las llamadas.
- Transmisión de medios. Formatea el audio, video, datos, flujo de control y mensajería transmitidos en la interfaz de la red. La transmisión de los medios recibe también le audio, vídeo datos flujos de control y mensajes desde la interfaz de la red.
- Còdecs de audio. Codifican la señal desde el equipo de audio para su transmisión y descodifica el código de audio entrante. Las funciones que se requieren incluyen la codificación y descodificación de voz G.711. de manera opcional, se puede soportar la codificación y descodificación G.711, G.723.1, G.728 y G.729.
- Interfaz de la red. Una interfaz basada en paquetes que pueden hacer servicios de unidifusión y multidifusión de extremo a extremo de protocolo para el control de transmisión (TCP) y el protocolo de datagrama de usuario (UDP).
- Còdecs de video. Es opcional pero si esta proporcionando, debe ser capas de codificar y descodificar video de acuerdo con el Quarter Comment Intermedite Format (QCIF) H.261.
- Canal de datos. Soporta aplicaciones como acceso s base de datos, transferencia de archivos y conferencias audiografias (la posibilidad de

modificar una imagen común sobre múltiples computadoras de usuario de forma simultánea).

El control de llamadas real y los mensajes de actividad se mueven a puertos efímeros después de configurar la llamada inicial. Pero 1720 es el puerto que se conoce para las llamadas H.323, H225 también especifica la utilización de los mensajes Q.932 para servicios suplementarios. Los siguientes mensajes Q.931 y Q.932 son los mensajes de señalización mas utilizados en las redes H.323:

- Setup. Un mensaje hacia delante enviado por una entidad H.323 que llama en un intento de establecer conexión con la entidad H.323 llamada. Este mensaje se envía en el puerto TCP 1720 de H.225.
- Call proceeding. Un mensaje hacia atrás mandado desde la entidad llamada a la entidad que llama para avisarle que los procedimientos de establecimiento de llamada se han iniciado.
- Alerting. Un mensaje hacia atrás enviado desde la entidad llamada a la entidad llamante indicando que la parte llamada ha respondido a la llamada. El mensaje de conexión puede contener la dirección de transporte UDP/IP para la señalización de control H.245.
- Release complete. Enviado por el punto final que inicia la conexión, que indica que la llamada ha sido liberada. Se puede enviar este mensaje únicamente si el canal de señalización de la llamada esta abierto o activo.
- Facility. Un mensaje Q.932 utilizado para solicitar o confirmar servicios complementarios. También se utiliza para indicar si una llamada debe ser dirigida o debe ir a través de un gatekeeper.

Se puede enrutar el canal de señalización en un red H.323 de dos maneras: a través de señalización de llamada directa de punto final (direct endpoint call signaling) y de señalización de llamada de gatekeeper enrutado (GKRCS, gatekeeper routed call signaling). En el método de señalización directa de punto final, los mensajes de señalización se envían directamente entre los dos puntos finales.

4.6.- TUNNELING H.245.

Se puede encapsular o “tunelizar” mensajes H.245 dentro del canal de señalización de llamadas H.225 en lugar de crear un canal de control H.245 separado. Este método mejora el tiempo de conexión de llamada y asignación de recursos, y proporciona una sincronización entre la señalización y el control de llamadas. Se pueden encapsular múltiples mensajes H.245 en un mensaje H.225. Asimismo, en cualquier momento un punto final puede conmutar con una conexión H.245 separada.

Procedimientos de conexión rápida. Los dos procedimientos para establecer canales de medios entre puntos finales son H.245 y fast connect. Fast connect permite que se establezca la conexión de medios para llamadas básicas punto a punto con un mensaje de intercambio de ida y vuelta. Estos procedimientos dictan que el punto final llamante incluye el elemento faststart (inicio rápido) en el mensaje de configuración inicial.
La parte faststart consiste en secuencias de canal lógico, capacidades de canal de medios y los parámetros para abrir e iniciar la transmisión de medios. En respuesta,

el punto final llamado devuelve un mensaje H.225 (call proceeding, progress, alerting o connect) que contiene un elemento faststart que selecciona las capacidades de terminal aceptadas. En ese momento, tanto los puntos finales llamantes como los llamados pueden transmitir medios si la secuencia de configuración en H.225 ha alcanzado el estado conectado.

4.7.- GATEWAY.

El gateway refleja las características de un punto final de una red de circuito conmutado (SCN) y un punto final H.323 traduce entre formatos de audio, video y transmisión de datos, así como un sistema de comunicación y protocolos. Esto incluye la configuración y el borrado de la llamada en la red IP y en la red SCN.
Los gateways no son necesarios a menos que se requiera la interconexión con la SCN. Por tanto, los puntos finales H.323 pueden comunicar directamente sobre la red de paquetes sin conectar con un gateway. El gateway actúa como un Terminal H.323 o MCU en la red y un Terminal SCN o MCU en la SCN,

4.8.- GATEKEEPER.

El gatekeeper es una función opcional que proporciona servicios de control de pre-llamada y nivel de llamada a los puntos finales H.323 los gatekeeper están lógicamente separados de los demás elementos de la red en su entorno H.323 si se implementa mas de un gatekeeper, se lleva a cabo la intercomunicación de una manera no especificada. En general, el propósito del gateway es reflejar transparentemente las características de un extremo en la red IP a otro en una red conmutada y viceversa.

El gatekeeper puede utilizar una simple secuencia de consulta/respuesta o location confirmation (LCF) para localizar a los usuarios remotos

Si un gatekeeper esta presente en un sistema H.323, debe llevar a cabo lo siguiente:

- Conversión de direcciones. Proporciona direcciones IP de punto final desde los alias H.323 (como pc1@cisco.com) o direcciones E164(numero de teléfono normal).
- Control de admisión. Proporciona acceso autorizad a H.323 utilizando los mensajes *admisión request/admisión confirm/admisión reject* (ARQ/ACF/ARJ).
- Control de ancho de banda. Consiste en la administración de los requisitos de ancho de banda utilizando los mensajes (BRQ/BCF/BRJ),
- Administración de zona. Para los terminales, gateways y MCU registrados; se explica en la sección “señalización RAS”.

4.9.- CONTROL DE ANCHO DE BANDA.

El control de ancho de banda esta limitado en cuanto al ámbito al gatekeeper y a los gateways y no tiene en cuenta el estado de la propia red. El gatekeeper solo mira en su ancho de banda estático para determinar si acepta o rechaza el ancho de banda solicitado.
El control de ancho de banda se administra inicialmente atreves del intercambio de administradores entre un punto final y un gatekeeper en una secuencia ARQ/ACF/ARJ. Sin embargo el ancho de banda puede cambiar durante una llamada. Podemos utilizar los siguientes mensajes para cambiar el ancho de banda:

- BRQ. Es enviado en un punto final al gatekeeper pidiendo un incremento o disminución en el ancho de banda de la llamada.
- BCF. Es enviado por el gatekeeper para confirmar la aceptación de la petición de cambio de ancho de banda.
- BRJ. Es enviado por el gatekeeper para rechazar la petición de cambio de ancho de banda (enviada si el ancho de banda solicitado no esta disponible).

4.10.- LA MCU Y SUS ELEMENTOS.

El controlador multipunto (MC) soporta conferencias entre tres o más puntos finales en una conferencia multipunto. Los MC transmiten el conjunto de capacidades para cada punto final en la conferencia multipunto y pueden recibir las capacidades durante las conferencias. La función MC puede residir en un Terminal, gateway, gatekeeper o MCU.

El procesador multipunto final que soporta conferencias multipunto y, por lo menos, consta de un MC y uno o más MP. Si soporta conferencias multipuntos centralizadas, la MCU típica consta de un MC. Un MP de audio, video y datos.

4.11.- CONTROLADOR MULTIPUNTO.

Un controlador multipunto es un componente de H.323 que provee capacidad de negociación con todos los terminales para llevar a cabo niveles de comunicaciones. También puede controlar recursos de conferencia tales como multicasting de vídeo. El Controlador Multipunto no ejecuta mezcla o conmutación de audio, vídeo o datos.

4.12.- PROCESADOR MULTIPUNTO.

Un procesador multipunto es un componente de H.323 de hardware y software especializado, mezcla, conmuta y procesa audio, vídeo y / o flujo de datos para los participantes de una conferencia multipunto de tal forma que los procesadores del terminal no sean pesadamente utilizados. El procesador multipunto puede procesar un flujo medio único o flujos medio múltiples dependiendo de la conferencia soportada.

4.13.- SERVIDOR PROXY H.323.

Es un Proxy específicamente diseñado para el protocolo H.323. el Proxy actúa en la capa de aplicación y puede examinar los paquetes entre dos aplicaciones que se comunican. Los Proxy pueden determinar el destino de una llamada y realizar la conexión si se desea. El Proxy soporta las siguientes funciones clave:

- Los terminales que no soportan el protocolo de reserva de recursos (RSVP) se puede conectar a través de un acceso o una red de área local (LAN) con una calidad de servicio (QoS) relativamente buena con el Proxy.
- Los praxis soportan el enrutamiento del trafico H.323 separados del trafico de datos ordinarios a través de un enrutamiento de aplicación especifico.
- Un Proxy es compatible con la conversión de dirección de red, permitiendo que los nodos H.323 sean desplegados en las redes con un espacio de dirección privado.
- Un Proxy desplegado sin un firewall o independientemente de un firewall proporciona seguridad, por lo que únicamente el trafico H.323 pasa por el mismo. Un Proxy desplegado junto con un firewall permite que el firewall sea configurado para pasar todo el trafico H.323 tratando el Proxy como si fura un nodo de confianza. Esto permite que el firewall proporciones la seguridad del networking de datos y que Proxy proporcione la seguridad H.323.

4.14.- CONJUNTO DEL PROTOCOLO H.323.

El conjunto del protocolo H.323 esta basado en varios protocolos, La familia de protocolos soporta la admisión de llamadas, la preparación, el estado, el borrado, los flujos del medio y los mensajes en los sistemas H.323 estos protocolos son soportados por mecanismos de entrega de paquetes seguros sobre las redes de datos.

El conjunto del protocolo H.323 esta dividido en tres áreas de control principales:

- Señalización de registro, admisiones y estado (RAS). Proporciona un control de prellamadas en las redes basadas en gatekepeer H.323.
- Señalización de control de llamadas. Se utiliza para conectar, mantener y desconectar llamadas entre puntos finales.
- Control y transporte de medios. proporciona el canal H.254 seguro de transportar los mensajes de control de los medios. El transporte ocurre con un flujo UDP no seguro.

4.15.- SEÑALIZACIÓN RAS.

La señalización RAS proporciona un control de prellamadas en las redes H.323 donde existen gatekeepers y una zona. El canal RAS se establece entre puntos finales y gatekeepers a través de una red IP. El canal RAS esta abierto antes de que ningún otro canal sea establecido y e independiente de la señalización de control de llamadas y de los Canals de transporte de medios. Esta conexión UDP no segura

transporta los mensajes RAS que realizan el registro, las admisiones, los cambios de ancho de banda, el estado y los procedimiento de desenganche.

El canal de señalización RAS es independiente del canal de señalización de llamada, y del canal de control H.245. . H.245 maneja mensajes de control de extremos a extremos entre cantidades H.323. Los procedimientos H.245 establecen canales lógicos para la transmisión de información de audio, video, datos y canal de control. Un punto final establece un canal H.245 para cada llamada con el punto final que esta particionado. El canal de control seguro se crea sobre IP utilizando el puerto TCP dinámicamente asignado en el último mensaje de señalización de llamada.

El intercambio de capacidades, la apertura y cierre de canales lógicos, los modos de preferencia y el control de los mensajes ocurren sobre este canal de control. H.245 también permite intercambio de capacidades separadas para la transmisión y recepción, así como la negociación de las funciones, como determinar que códec se utilizara.
Si utilizamos la señalización de las llamadas de gatekeeper enrutado, podemos controlar el enrutamiento del canal de dos maneras: utilizar Direct H.245 Control, que tiene lugar directamente entre dos puntos finales participantes, o bien utilizar gatekeeper routed H.245 control, que tiene lugar entre cada punto final y su gatekeeper.
Podemos hacer uso de los siguientes procedimientos y mensajes para permitir la operación de control H.245:

- Capability Exchange. Consiste en un mensaje que intercambian de manera segura las capacidades entre dos puntos finales, también llamados terminales. Estos mensajes indican capacidades del terminador para transmitir y recibir audio, video y datos al terminal que esta particionado. Para audio, el intercambio de capacidades incluye codecs de transcodificacion de voz de la serie G, como G.729 a 8 kbps, G.728 a 16 kbps, G.711 a 64 kbps, G.723 a 5,3 o 6,3 kbps, o G.722 a 48, 56 y 64 kbps. También incluyen la velocidad de muestreo de las series de la International Organization for Standardization (ISO) IS.111723 con 32, 44,1 y 48 KHz e IS.13818-3 con 16, 22,05, 24, 32, 44,1 y 48 KHz; así como los codecs de audio de voz de tasa completa, tasa media y tasa mejorada de GSM.

- Master-slave termination. Procedimientos utilizados que punto final es el principal (maestro) y que punto final es el secundario (esclavo) para una llamada determinada. La relación se mantiene durante la duración de la llamada y se utilizara para resolver conflictos entre puntos finales. Las reglas maestro-esclavo (master-slave) se utilizan cuando ambos puntos finales solicitan acciones similares a la vez.

- Round-trip delay (retraso de ida y vuelta) procedimiento utilizado para determinar el retraso entre los pintos finales de origen y de terminación. El mensaje Round-trip delayRequest mide el retraso y verifica si la entidad retoma del protocolo H.245 esta activa.

- Logical channel signaling. Abre y cierra el canal lógico que transporta la información de audio, video y datos. El canal se prepara antes de la transmisión real para asegurar que los terminales están preparados y son capaces de recibir y descodificar información. Los mismos mensajes de señalización establecen los canales unidireccionales y bidireccionales. Cuando se ha establecido la señalización de canal lógico con éxito, el puerto UDP para el canal de medios RTP es pasado desde el punto final de terminación hasta el punto final de origen. Asimismo, cuando se utiliza el modelo gatekeeper call routed, es en este punto donde el gatekeeper puede desviar los flujos RTP proporcionando la dirección UDP/IP real del punto final de terminación.

Los procedimientos de apertura de canal lógico H.245 no se utilizan para establecer el canal de señalización RAS. El canal de señalización RAS se abre antes de que se establezca cualquier otro canal entre puntos extremos H.323.

El servicio de extremo a extremo no fiable (UDP, IPX) es obligatorio para los canales de audio, los canales de video y el canal de RAS. Estos servicios pueden ser dúplex o símplex y de unicast o multicast dependiendo de la aplicación, las capacidades de los terminales y la configuración de la red.

DESCUBIRMIENTO DEL GATEKEEPER. Es un proceso manual o automático que los puntos utilizan para identificar con que gatekeeper registrarse. El método manual, los puntos finales están configurados con la dirección IP del gatekepeer, por lo tanto, puede intentar el registro inmediatamente, pero únicamente con el gatekeeper preferido. El método automático permite que la relación entre puntos finales y gatekeepers cambie a lo largo del tiempo y requiere un mecanismo conocido como autodescubrimiento.

El autodescubrimiento permite que un punto final que tal vez no conozca a su gatekeeper, pueda descubrirlo a través de un mensaje de multifunción.

4.16.- REGISTRO.

Es el proceso que permite que los gateways, puntos finales y MCU alcancen una zona e informen al gatekeeper de sus direcciones IP y alias. El registro, que es un proceso necesario, ocurre después del proceso de descubrimiento, pero antes que se intente realizar ninguna llamada

4.17.- LOCALIZACIÓN DEL PUNTO FINAL.

Los puntos finales y gateways utilizan la localización de punto final para obtener información de contacto cuando solo esta disponible la información de alias. Los mensajes locate (localizar) son enviados a la dirección de canal RAS del gatekeeper o son multidifundidos a la dirección de difusión de descubrimiento del gatekeeper

El punto final o gatekeeper puede incluir una o más direcciones E164 fuera de la zona en la petición.

4.18.- ADMISIONES.

Los mensajes de admisión entre puntos finales y gatekeepers proporcionan las bases para la admisión de llamadas y control de ancho de banda. Los gatekeepers autorizan el acceso a las redes H.323 confirmando o rechazando una petición de admisión. Una petición de admisión incluye el ancho de banda solicitado, que puede ser reducida por el gatekeeper en la confirmación.

4.19.- PROTOCOLOS.

Es el lenguaje que utilizarán los distintos dispositivos VoIP para su conexión. Esta parte es muy importante ya que de ella dependerá la eficacia y la complejidad de la comunicación.

Por orden de antigüedad (de más antiguo a más nuevo):

- H.323 - Protocolo definido por la ITU-T.
- SIP - Protocolo definido por la IETF.
- Megaco (También conocido como H.248) y MGCP- Protocolos de control.
- Skinny Client Control Protocol - Protocolo propiedad de Cisco.
- MiNet - Protocolo propiedad de Mitel.
- CorNet-IP - Protocolo propiedad de Siemens.
- IAX.
- Skype - Protocolo propietario peer-to-peer utilizado en la aplicación Skype.
- IAX2.
- Jingle - Protocolo abierto utilizado en tecnología Jabber.

VOIP Y SUS PROTOCOLOS. Voz sobre Protocolo de Internet, también llamado Voz sobre IP, VoIP, Telefonía IP, Telefonía por Internet, Telefonía Broadband y Voz sobre Broadband es el enrutamiento de conversaciones de voz sobre Internet o a través de alguna otra red basada en IP.

Los Protocolos que son usados para llevar las señales de voz sobre la red IP son comúnmente referidos como protocolos de Voz sobre IP o protocolos IP. Ellos pueden ser vistos como implementaciones comerciales de la Red experimental de Protocolo de Voz (1973) inventado por ARPANET.

El tráfico de Voz sobre IP puede ser llevado por cualquier red IP, incluyendo aquellas conectadas a la red de Internet, como por ejemplo en una red de área local (LAN).

PROTOCOLOS DE INICIO DE LA SESIÓN. El protocolo de inicio de la sesión (SIP) es un protocolo de control de señalización de la capa de aplicación que se utiliza para establecer, mantener y terminar sesione multimedia. Las sesiones multimedia incluyen la telefonía internet, las conferencias y otras aplicaciones similares que proporcionan medios como audio, video y datos.
Se pueden utilizar invitaciones SIP para establecer sesiones y transportar descripciones de la sesión. SIP soporta sesiones unidifusión y multidifusión, así

como llamadas punto a punto y multipunto. Las comunicaciones se pueden establecer y terminar utilizando estas cinco facetas del SIP: localización del usuario, capacidad del usuario, disponibilidad de usuario, configuración de llamada y manejo de la llamada.
SIP, es en el que se basa la petición de comentarios (RFC) 2543, es un protocolo basado en texto que es parte de la arquitectura multimedia general del grupo IETF (internet engincering task force). El IEF incluye también el protocolo de reserva de recursos (RSVP, resource reservation protocol; RFC 2205), el protocolo de transporte en tiempo real (RTP, real-time transport protocol; RFC 1889), el protocolo de streaming en tiempo real (RTSP, real-time streaming protocol; RFC 2326), el protocolo de anuncio de la sesión (SAP, sesión announcement protocol, borrador de internet) y el protocolo de descripción de la sesión (SDP, sesión description protocol; RFC 2327). Sin embargo las funciones del SIP son independientes, por lo que no dependen de ninguno de estos protocolos. Es importante tomar nota de que el SIP puede operar en conjunto con otros protocolos de señalización, como el H.323.
La telefonía de protocolo de internet (IP) se sigue desarrollando y en el futuro requerirá posibilidades adicionales de señalización incremental. Las cabeceras de los mensajes SIP son versátiles y se pueden registrar funciones adicionales como la agencia de asignación de números de internet (IANA, internet assigned numbers authority). La flexibilidad del mensaje SIP también permite que los elementos construyan servicios telefónicos avanzados, incluidos los servicios de tipo de movilidad.

4.20.- PROTOCOLO DE INICIO DE LA SESIÓN SIP.

VISIÓN GENERAL DE SIP. Los dos componentes de un sistema SIP son los agentes de usuario y los servidores de red. Las partes que llaman y son llamadas se identifican con direcciones SIP; las partes necesitan localizar servidores y usuarios.

AGENTES DE USUARIO. Los agentes de usuario son aplicaciones cliente de sistema final que contienen un cliente usuario-agente (UAC) y un servidor usuario-agente (UAS), también conocidos como cliente y servidor, respectivamente.

Cliente. Inicia las peticiones SIP y actúa como el agente usuario del llamante.
Servidor. Recibe las peticiones y devuelve las respuestas en nombre del usuario; actúa como el agente de usuario llamado.

SERVIDORES DE RED. Existen dos tipos de servidores de red SIP: los servidores proxy y los servidores redirec (de dirección).

Servidor proxy. Actúa en nombre de otros clientes y contiene funciones del cliente y de servidor. Un servidor proxy interpreta y puede rescribir cabeceras de peticiones antes de pasarlas a los demás servidores. Rescribir las cabeceras identifica al proxy como el indicador de la petición y asegura que las respuestas siguen la misma ruta de vuelta hasta el proxy en lugar de hasta el cliente.

Servidor de redirección. Acepta las peticiones SIP y envía una respuesta redirigida al cliente que contiene la dirección del siguiente servidor. Los servidores de redirección no aceptan llamadas ni tampoco procesan o reenvían peticiones SIP.

DIRECCIONAMIENTO. Las direcciones SIP, también llamadas localizadores universales de recursos (URL) IP, existen en la forma de usuarios @ hosts. Similar a una dirección de correo electrónico, un URL SIP se identifica por usuarios@host. La parte de usuario de la dirección puede ser un nombre de usuario o un número de teléfono, y la parte de host puede ser un nombre de dominio o una dirección de red. Se puede identificar un URL SIP de un usuario por su dirección de correo electrónico. Estos ejemplos muestran dos posibles direcciones URL SIP:

sip:ciscopress@cisco.com
sip:4085262222@171.171.171.1

LOCALIZACIÓN DE UN SERVIDOR. Un cliente puede enviar una petición SIP directamente a un servidor proxy configurado localmente, o bien a la dirección IP y puerto del correspondiente URLSIP. Enviar una petición SIP es relativamente fácil, ya que la aplicación de sistema final conoce al servidor proxy. Enviar una petición SIP de la segunda manera es algo mas complicado.

4.21.- TRANSACCIONES SIP.

Cuando se ha resuelto el tema de dirección, el cliente envía una o más peticiones SIP y recibe una o más peticiones y respuestas asociadas con esa actividad están consideradas como parte de una transacción SIP. Para una mayor simplicidad y coherencia, los campos de cabecera en todos los mensajes de petición coinciden con los campos de cabecera en todos los mensajes de respuesta.

Se pueden transmitir transacciones SIP en los protocolos UDP y TCP.

4.22.- LOCALIZACIÓN DE UN USUARIO.

La parte llamada pude desplazarse desde uno o varios sistemas finales a lo largo del tiempo. Puede moverse desde la red de área local corporativa a una oficina encasa conectada a través de su proveedor de servicios de Internet (ISP) o a una conexión pública Internet mientras atiende una conferencia. Por tanto, para los servicios de localización, SIP necesita acomodar la flexibilidad y la movilidad de los sistemas finales IP. Las localizaciones de estos sistemas finales pueden estar registradas con el servidor SIP o con otros servidores de localización fuera del ámbito de SIP. En este último caso, el servidor SIP almacena la lista de localizaciones basadas en el servidor de localización exterior que esta devolviendo múltiples posibilidades de host.

La acción y resultado de localizar aun usuario depende del servidor SIP que se esté utilizando. Un servidor de la dirección simplemente devuelve la lista completa de localizaciones y permite que el cliente localice directamente al usuario. Un servidor proxy puede probar las direcciones en paralelo hasta que la llamada tenga éxito.

4.23.- MENSAJES SIP.

Existen dos tipos de mensaje SIP: peticiones iniciadas por los clientes y respuestas devueltas desde los servidores. SIP es un protocolo basado en texto con una sintaxis de mensaje y campos de cabecera idénticos al protocolo de transferencia de IP al texto (HTTP). Los mensajes SIP se envían sobre los protocolos TCP o UDP con múltiples mensajes transportados en una única conexión TCP o datagrama UDP.

CABECERAS DE MENSAJE. Las cabeceras de mensaje se utilizan para especificar la parte llamante, la parte llamada, la ruta y el tipo de mensaje de una llamada. Los cuatros grupos de cabeceras de mensaje son los siguientes.

Cabeceras Generales. Se aplica a las peticiones y a las respuestas.
Cabeceras de Entidad. Define información sobre el tipo del cuerpo del mensaje y longitud.
Cabeceras de Petición. Permite que el cliente incluya información de petición adicional.
Cabeceras de Respuesta. Permite que el servidor incluya información de respuesta adicional.

PETICIONES DE MENSAJE. La comunicación SIP presenta seis tipos de peticiones de mensaje:

INVITE. Este método indica que el usuario o servicio es invitado a participar en una sesión. Incluye una descripción de sesión, y para llamadas de dos vías, la parte llamante indica el tipo de medio.

ACK. Representan la confirmación final por parte del sistema final y concluye la transacción iniciada por el comando INVITE.

OPTIONS. Este método permite consultar y reunir posibilidades de agentes de usuarios y servidores de red.
BYE. Este método se utiliza por las partes que llaman y son llamadas para liberar una llamada.

CANCEL. Esta petición permite que los agentes de usuarios y servidores de red, cancelen cualquier petición que este progreso.

REGISTER. Este método se utiliza por los clientes para registrar información de localización con los servidores SIP.

4.24.- PLAN DE MARCACIÓN.

Arquitectura del plan de marcación: La arquitectura del plan de marcación se divide en dos tipos: las rutas externas, que se refieren a todas las llamadas fuera del CallManager; y las rutas internas, que se refieren a todas las llamadas dentro del CallManager.

*Rutas Externas: E*n el caso del modelo de procesamiento de llamada centralizado, las rutas externas abarcan sólo las llamadas hacia teléfonos fuera de la empresa, y no a llamadas entre campus, por lo tanto todas las llamadas de rutas externas se realizan a través de la PSTN. Existen tres formas de proveer acceso hacia la red telefónica pública conmutada en un modelo con procesamiento de llamada centralizada: plan de marcación centralizado, donde todas las llamadas hacia la PSTN se realizan a través del sitio central; plan de marcación distribuido, donde cada sitio posee su propio gateway y enlace hacia la PSTN; y plan de marcación híbrido, algunos sitios remotos dependen del sitio central y otros poseen su propio gateway.

Los planes de marcación centralizada y marcación híbrida, consumen mayor ancho de banda del enlace WAN y requieren gateways con mayor capacidad, encareciendo la implementación del diseño, por esto, se elige el plan de marcación distribuido con procesamiento de llamada centralizada para el diseño de la red telefónica IP. La configuración del plan de marcación utiliza patrones de rutas, que definen cuándo una llamada tiene como destino la PSTN y si es una llamada local, larga distancia nacional, larga distancia internacional, a celulares o a números especiales. Cuando el usuario marca el número de teléfono el CallManager manipula los dígitos y envía la llamada al gateway local que se encarga de mandar la llamada por el enlace PSTN. Existen restricciones de llamadas, las cuales se configuran en el CallManager utilizando dos elementos: Los espacios de búsqueda de llamada y las particiones. Una partición es un grupo de dispositivos con accesibilidad similar y un espacio de búsqueda de llamada define cuales particiones son accesibles a un dispositivo en particular. Los dispositivos asignados a un cierto espacio de búsqueda de llamada pueden acceder sólo a las particiones pertenecientes a ese espacio y cualquier llamada que intenten fuera de él serán rechazadas devolviendo un tono de ocupado al usuario. Cada partición se define como un subconjunto del directorio, es decir un grupo de números de directorio (DN).

Rutas Internas: La marcación entre los sitios remotos debe requerir solamente el número interno de la extensión, para esto:

- Todos los teléfonos IP deben pertenecer a una misma partición dentro del cluster, la cual puede ser alcanzada desde todos los espacios de búsqueda de llamada de los sitios remotos.

- Cada sitio remoto debe tener su propio conjunto de particiones y patrones de rutas y el número de particiones por sitio remoto depende del número de políticas restrictivas asociadas con los patrones de rutas.

- Cada sitio remoto debe tener sus propios espacios de búsqueda de llamada para los teléfonos IP, y se asocian a las particiones del cluster y a los patrones de rutas locales. Se establecen cuatro tipos de particiones, que son: llamadas locales y números de emergencia, llamadas larga distancia nacional, llamadas larga distancia internacional y llamadas a celulares. Existen cuatro tipos de políticas restrictivas: los que pueden llamar a todos los destinos; los que sólo pueden hacer llamadas locales y de emergencia; los que sólo pueden hacer llamadas locales, de emergencia y a celulares; y los que sólo pueden hacer llamadas locales, de emergencia, a celulares y larga distancia nacional. Existen dos formas de enrutar las llamadas entre sitios remotos dentro de un CallManager, a través de la IP WAN y a través de la PSTN. Las llamadas que se realicen entre sitios deben elegir el enlace WAN como primera opción, sin embargo, en caso que el ancho de banda del enlace WAN no sea suficiente para establecer una nueva llamada, ésta se enviará a través de la PSTN en forma transparente al usuario, lo que se logra usando el enrutamiento alternativo automático (AAR, Automated alternate routing). Este mecanismo habilita al CallManager para establecer un camino alternativo cuando los medios de voz primarios (IP WAN) entre dos dispositivos finales dentro del cluster no tienen ancho de banda disponible.

Procesador de llamadas: Anteriormente se estableció que el procesamiento de llamadas del diseño lo realiza el software Cisco CallManager 3.3, sin embargo la plataforma del procesador depende de los tipos de servidores y el peso de los dispositivos registrados en ellos.

Existen tres tipos de plataformas o servidores:

- Servidor estándar: Posee un solo procesador, una fuente de alimentación y no tiene disco duro de respaldo.

- Servidor estándar de alta disponibilidad: Posee un procesador, múltiples fuentes de alimentación y no tiene disco duro de respaldo.

- Servidor de alta funcionalidad: Posee múltiples procesadores, múltiples fuentes de alimentación y múltiples arreglos de disco duro de respaldo.

Debido a que el procesador se implementa en un cluster, no es necesario que cada plataforma posea discos de respaldo, por lo tanto considerando la mejor relación costo beneficio, el diseño utiliza un servidor estándar de alta disponibilidad.

El cluster se conforma de:

- Un servidor TFTP y editor de base de datos: Donde el servidor TFTP posee los archivos de configuración de los dispositivos de voz, y el editor de base de datos posee todos los cambios de configuración y graba los detalles de las llamadas.

Arquitectura de red convergente: El diseño de la red convergente se puede explicar mediante un modelo de cuatro capas:

- Capa de acceso: Describe los dispositivos por los cuales los usuarios acceden a la red y los switches a los cuales se conectan. Los switches de esta capa deben proveer alimentación sobre ethernet, poseer convergencia rápida, soportar múltiples colas y el estándar 802.1q para el uso de VLAN.

- Capa de distribución y capa núcleo: En estas capas se encuentran los switches que conectan la capa de acceso y el gateway. Los switches de esta capa deben soportar múltiples colas, estándar 802.1q y realizar clasificación y reclasificación del tráfico.

- Agregación de la WAN: Esta capa contiene los gateways de los diferentes campus, los cuales deben soportar múltiples colas, estándar 802.1q, realizar clasificación y reclasificación del tráfico, y soportar H.323 para ofrecer procesamiento de llamadas en los sitios remotos en caso que falle el enlace WAN.

4.25.- DISEÑO DE UNA RED DE TELEFONIA BASADA EN VoIP

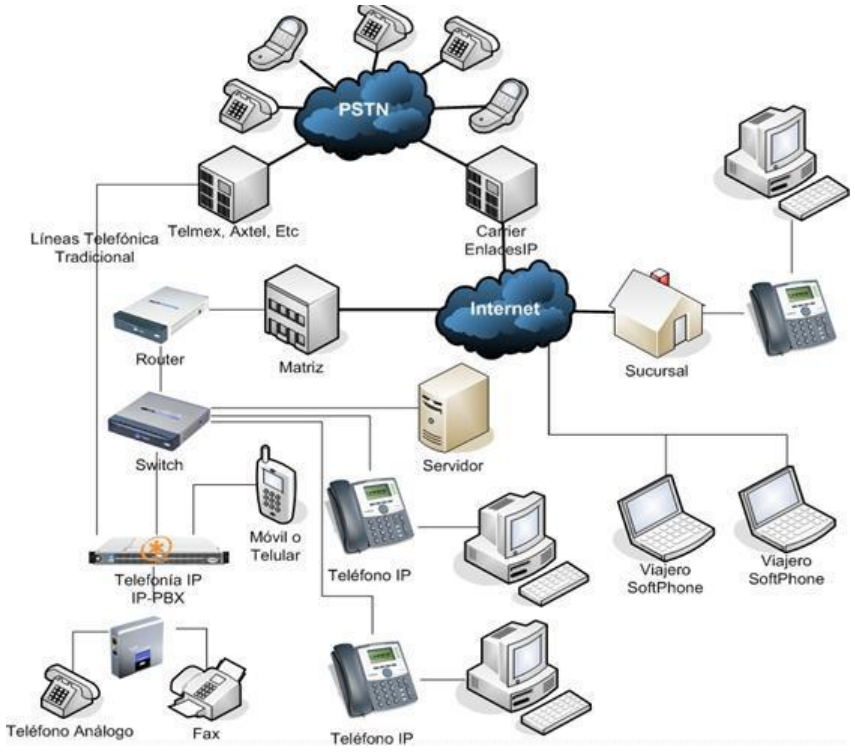


Fig.20.- Red basada en VoIP

TELEFONIA VOIP. La línea Telefónica IP se conecta a cualquier Internet de banda ancha para realizar la comunicación con las líneas telefónicas tradicionales, y así entablar el enlace entre el usuario y su destinatario.

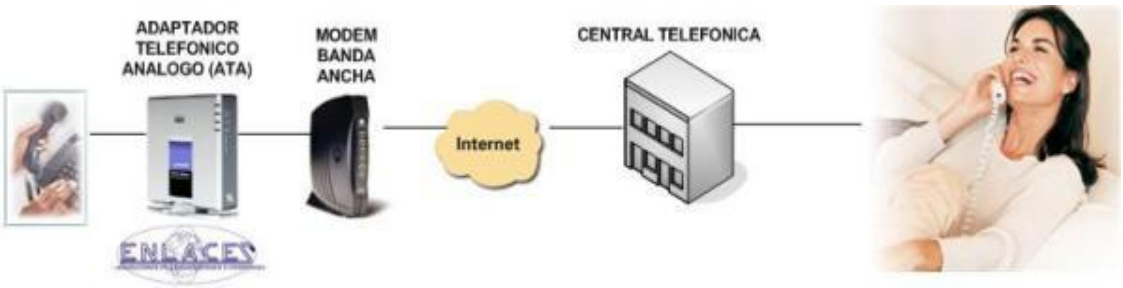


Fig.21.-Telefonía VoIP

De la misma manera como se muestra, el adaptador es conectado al módem de banda ancha, pasa por el Internet y realiza la conexión con las centrales telefónicas del país correspondiente, enviando la llamada con el destinatario. Todo este proceso e interconexión sucede en tan solo un par de segundos.

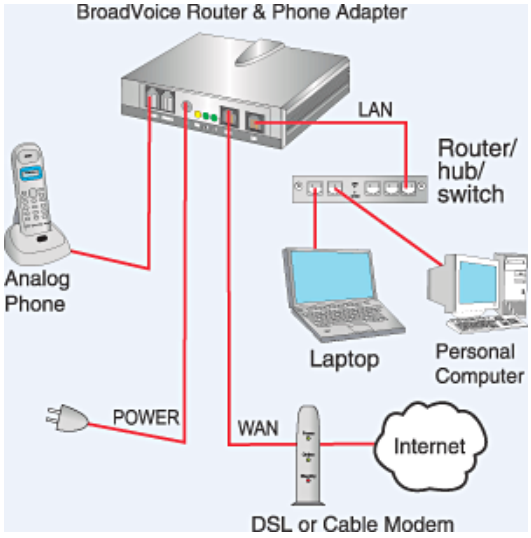


Fig.22.- Adaptador telefónico IP

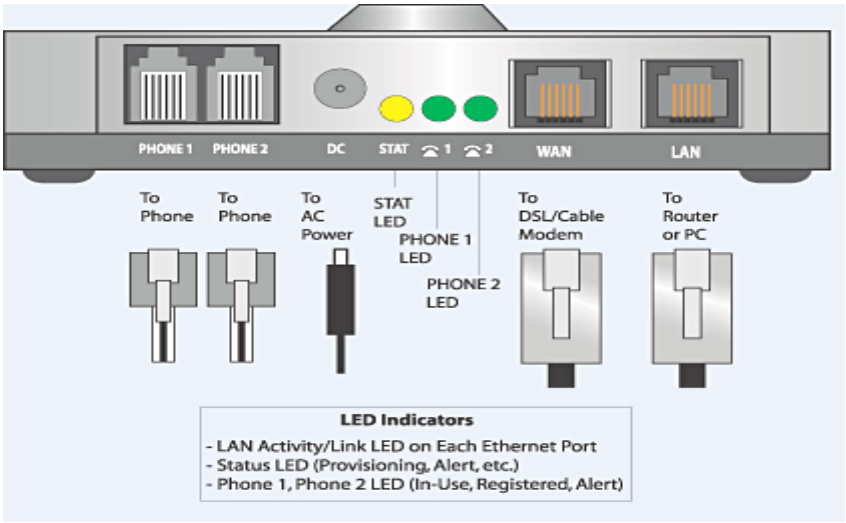


Fig.23.- Componentes para una conexión VoIP

COSTO. En general, el servicio de telefonía vía VoIP es gratuito o cuesta muchísimo menos que el servicio equivalente tradicional y similar a la alternativa que los proveedores del servicio de la Red Pública Telefónica Conmutada (PSTN) ofrecen. Algunos ahorros en el costo son debidos a utilizar una misma red para llevar voz y datos, especialmente cuando los usuarios tienen sin utilizar toda la capacidad de una red ya existente la cual pueden usar para VoIP sin un costo adicional. Las llamadas de VoIP a VoIP entre cualquier proveedor son generalmente gratis, en contraste con las llamadas de VoIP a PSTN que generalmente cuestan al usuario de VoIP.

Hay dos tipos de servicio de PSTN a VoIP: Llamadas Locales Directas (Direct Inward Dialling: DID) y Números de acceso. DID conecta a quien hace la llamada directamente al usuario VoIP mientras que los Números de Acceso requieren que este introduzca el número de extensión del usuario de VoIP. Los Números de acceso son usualmente cobrados como una llamada local para quien hizo la llamada desde la PSTN y gratis para el usuario de VoIP.

4.26.- FUNCIONALIDAD.

VoIP puede facilitar tareas que serían más difíciles de realizar usando las redes telefónicas tradicionales:

- Las llamadas telefónicas locales pueden ser automáticamente enrutadas a tu teléfono VoIP, sin importar en donde estés conectado a la red. Lleva contigo tu teléfono VoIP en un viaje, y donde quiera que estés conectado a Internet, podrás recibir llamadas.
- Números telefónicos gratuitos para usar con VoIP están disponibles en Estados Unidos de América, Reino Unido y otros países de organizaciones como Usuario VoIP.
- Los agentes de Call center usando teléfonos VoIP pueden trabajar en cualquier lugar con conexión a Internet lo suficientemente rápida.
- Algunos paquetes de VoIP incluyen los servicios extra por los que PSTN (Red Telefónica Conmutada) normalmente cobra un cargo extra, o que no se encuentran disponibles en algunos países, como son las llamadas de 3 a la vez, retorno de llamada, remarcación automática, o identificación de llamadas.

4.27.- MOVILIDAD.

Los usuarios de VoIP pueden viajar a cualquier lugar en el mundo y seguir haciendo y recibiendo llamadas de la siguiente forma:

Los subscriptores de los servicios de las líneas telefónicas pueden hacer y recibir llamadas locales fuera de su localidad. Por ejemplo, si un usuario tiene un número telefónico en la ciudad de Nueva York y está viajando por Europa y alguien llama a su número telefónico, esta se recibirá en Europa. Además si una llamada es hecha de Europa a Nueva York, esta será cobrada como llamada local, por supuesto, debe de haber una conexión a Internet disponible, como WiFi para hacer esto posible.

Los usuarios de Mensajería Instantánea basada en servicios de VoIP pueden también viajar a cualquier lugar del mundo y hacer y recibir llamadas telefónicas.

Los teléfonos VoIP pueden integrarse con otros servicios disponibles en Internet, incluyendo video llamadas, intercambio de datos y mensajes con otros servicios en paralelo con la conversación, audio conferencias, administración de libros de direcciones e intercambio de información con otros (amigos, compañeros, etc.).

4.28.- TERMINACIÓN DE LLAMADA.

Cualquier punto final que participe en una llamada puede iniciar el procedimiento de terminación de llamada. En primer lugar, deben cesar las transmisiones de medios (como audio, video o datos) y cerrarse todos los canales lógicos. A continuación, debe finalizar la sesión H.245 y enviar un mensaje de liberación completa (release complete message) en el canal de señalización de llamada, si sigue estando abierto o activo. En este momento, si ningún gatekeeper esta presente, se termina la llamada. Cuando un gatekeeper esta presente, se utilizan los siguientes mensajes en el canal RAS para completar la terminación de llamadas:

- Disengage Request (DRQ). Se envía por un punto final o gatekeeper para terminar una llamada.
- Disengage Confirm (DCF). Se envía por un punto final o gatekeeper para confirmar la desconexión de la llamada.
- Disengage Rejct (DRJ). Se envía por el punto final o gatekeeper para rechazar la desconexión de la llamada.

IP NO ES UN SERVICIO ES UNA TECNOLOGÍA. En muchos países del mundo, IP ha generado múltiples discordias, entre lo territorial y lo legal sobre esta tecnología, está claro y debe quedar claro que IP no es un servicio TPBLC, es un protocolo que se usa para empaquetar datos con una grado de eficiencia alto. Es tarea de la autoridad competente la regulación en la materia.

Como hemos visto VoIP presenta una gran cantidad de ventajas, tanto para las empresas como para los usuarios comunes. La pregunta sería ¿por qué no se ha implantado aún esta tecnología? A continuación analizaremos los aparentes motivos, por los que VoIP aún no se ha impuesto a las telefonías convencionales.

PARÁMETROS DE LA VOIP. Este es el principal problema que presenta hoy en día la penetración tanto de VoIP como de todas las aplicaciones de IP. Garantizar la calidad de servicio sobre una red IP, por medio de retardos y ancho de banda, actualmente no es posible; por eso, se presentan diversos problemas en cuanto a garantizar la calidad del servicio.

4.29.- CÓDECS.

La voz ha de codificarse para poder ser transmitida por la red IP. Para ello se hace uso de Códecs que garanticen la codificación y compresión del audio o del video

para su posterior decodificación y descompresión antes de poder generar un sonido o imagen utilizable. Según el Códec utilizado en la transmisión, se utilizará más o menos ancho de banda. La cantidad de ancho de banda suele ser directamente proporcional a la calidad de los datos transmitidos.

Entre los códecs utilizados en VoIP encontramos los G.711, G.723.1 y el G.729 (especificados por la ITU-T)

G.711 es un estándar de la ITU-T (Union Internacional de Telecomunicaciones) para la compresión de audio. Este estándar es usado principalmente en telefonía, y fue liberado para su uso en el año 1972.

G.711 es un estándar para representar señales de audio con frecuencias de la voz humana, mediante muestras comprimidas de la técnica de modulación PCM (Pulse Code Modulation), con una taza de muestreo de 8KHz y 8 bits por muestra. El codificador G.711 proporcionará un flujo de datos de 64Kbps

Para este estándar existen dos algoritmos principales, el *u-law*(usado en Norte América y Japón) y el *a-law*(usado en Europa y el resto del mundo)

Ambos algoritmos son logarítmicos, pero el *a-law* fue específicamente diseñado para ser implementado en una computadora.

El estándar también define un código para secuencia de repetición de valores, el cual define el nivel de potencia de 0 dB

RETARDO O LATENCIA. Una vez establecidos los retardos de procesado, retardos de tránsito y el retardo de procesado la conversación se considera aceptable por debajo de los 150 ms.

CALIDAD DEL SERVICIO. La calidad de servicio se está logrando en base a los siguientes criterios:

La supresión de silencios, otorga más eficiencia a la hora de realizar una transmisión de voz, ya que se aprovecha mejor el ancho de banda al transmitir menos información.

4.30.- COMPRESIÓN DE CABECERAS APLICANDO LOS ESTÁNDARES RTP/RTCP.

Priorización de los paquetes que requieran menor latencia. Las tendencias actuales son:CQ (Custom Queuing) (Sánchez J.M:, VoIP'99): Asigna un porcentaje del ancho de banda disponible.PQ (Priority Queuing) (Sánchez J.M:, VoIP'99): Establece prioridad en las colas.WFQ (Weight Fair Queuing) (Sánchez J.M:, VoIP'99): Se asigna la prioridad al tráfico de menos carga.DiffServ: Evita tablas de encaminados intermedios y establece decisiones de rutas por paquete.

La implantación de IPv6 que proporciona mayor espacio de direccionamiento y la posibilidad de tunneling.

Transporte de medios (RTP/RTCP). RTP proporciona transporte de medios en H.323. De manera mas especifica, RTP permite la entrega de extremo a extremo en tiempo real de audio, video y datos interactivos sobre las redes de unidifusión o multidifusión. Los servicios de empaquetamiento y transmisión incluyen la identificación de carga útil, la secuenciación, la marca de temporización y la monitorización.
RTP depende de otros mecanismos y de las capas bajas para asegurar la entrega a tiempo , la reserva de recursos, la fiabilidad y la QoS. RTCP monitoriza la entrega de datos y controla e identifica los servicios. El canal de medios se crea utilizando UDP, donde los flujos RTP actúan en un numero de puerto par y el flujo RTCP correspondiente actual en el siguiente numero de puertos mas alto (impar).

4.31.- COMPONENTES DEL SISTEMA CISCO IPC EXPRESS.

Esta sección trata en detalle los componentes de un sistema Cisco IPC Express, como ya se comento anteriormente, este sistema incluye el Software de procesamiento de llamada Cisco SME, la plataforma IP comunication y las aplicaciones y puntos finales IP.

4.32.- CISCO CALLMANEGER EXPRESS.

Cisco CME es un sistema de procesamiento de llamada basado en el Cisco IOS que ofrece un amplio abanico de opciones de telefonía IP para negocios de pequeño y mediano tamaño y para oficina troncales hasta 240 usuarios. Cuanta con una sección dedicada a la telefonía tradicional junto con otras más avanzadas que no se encuentran en la mayoría de soluciones de telefonía tradicionales. Las empresas pueden escoger también entre los modos de operación por sistema clave y PBX, o una combinación de ambos, en una única red.

Ya que Cisco CME es un software de procesamiento de llamadas totalmente basado en tecnología IP, su diseño no tiene restricciones de conexión física. Esto significa que puede configurar numerosos teléfonos y combinaciones de troncales PSTN (red telefónica conmutada pública, public Switched Telphone Network), en Cisco CME, ofreciendo un gran número de aplicaciones a las empresas. Por ejemplo, el grupo de búsqueda (Huntgroup), permite programar varios teléfonos de la empresa de modos que suene de modo secuencial. En otras palabras, cuando el primer teléfono esté ocupado o recibiendo una llamada, ésta pasará al siguiente de la secuencia, y así sucesivamente. En una empresa con mucha actividad, el grupo de búsqueda o la línea/multilínea compartida ofrecen muchas posibilidades de que ninguna llamada quede sin contestar.

La instalación inicia de disco SME se hace sencilla a través del sistema del asistente de configuración. Esta herramienta de configuración le hace una serie de preguntas para configurar el sistema del modo más eficiente posible. Los buzones de voz pueden incorporarse también de manera sencilla a través del asistente de inicialización Cisco UE.
Para la administración y configuración diaria, Cisco CME ofrece la posibilidad de usar una GUI web o la CLI (Interfaz de línea de comando, Command-Line Interface), del Cisco IOS. Este ultimo es el mismo Software empleado para configura Routers,

Suites y las plataformas. Para la plantilla no cualificada, la GUI web es la forma más sencilla de añadir usuarios, teléfonos extensiones, o realizar cualquier modificación en la configuración.

Cisco CME esta disponible mediante la compra de una licencia Cisco CME con la versión de los IOS de Cisco de router. El apéndice A resume todas estas características.

4.33.- PLATAFORMAS DE COMUNICACIONES IP.

Cisco CME funciona en las plataformas Cisco IPC Express, incluyendo la series Cisco 1700, 2600XM, 2691 y 3700 Access Router, así como las series Cisco 2800 y 3800 ISR. Estas plataformas de comunicación ofrecen una variedad de interfaces troncales PSTN tanto analógicas como digitales, interfaces de estación analógica y ranuras de estación analógicas y ranuras de extensión modulares en la que se pueden añadir un gran variedad de posibilidades, como conmutación integrada, aceleración VPN por hardware, correo de voz y sistemas de detección de intrusiones. Dependiendo del número de usuarios de la oficina, el tamaño de la plataforma de comunicaciones IP puede encargarse de llevar a cabo el enrutamiento, la conmutación, seguridad y otros servicios.

Las empresas que ya utilicen routers de acceso, o ISRs, para sus conectividades de datos pueden implantar Cisco IPC Express en estas plataformas con toda facilidad. Por otro lado, las que se hayan decantado por la telefonía IP pueden adquirir un paquete que incluye la plataforma, el software, las licencias y las aplicaciones. Ya que las plataformas proporcionan un amplio rango de soluciones en un único chasis, resulta fácil de administrar y configurar.

Las plataformas Cisco IPC Express disponen de un alto grado de modularidad. Las tarjetas utilizadas para aplicaciones de valor añadido o para conectividad pueden utilizarse para todo el catálogo de routers. Además, si un negocio supera un despliegue Cisco IPC Express y decide migrar el sistema a Cisco CallManager, tanto el equipamiento como las licencias adquiridas pueden utilizarse en dicha migración, preservándose así toda la inversión.

El catálogo sin plataformas Cisco IPC Express dispone de una gran capacidad de enrutamiento, soporte para teléfonos IP y opciones de densidad troncal PSTN para cumplir las necesidades de cualquier oficina pequeña o mediana. Las series Cisco 1700 y Cisco 2801 tienen la menor densidad de servicios, ofrecen conectividad modular u servicios de voz a nivel de entrada. Las series 2600XM, 2691 y 2800 ofrecen conectividad modular extendida. Las plataformas Cisco 3700 y 3800 son las que mejor rendimiento y servicio ofrecen. Todas ellas soportan el software Cisco IOS.

SERIES CISCO 1700. Las series Cisco 1700 están dirigidas a pequeñas empresas. Las plataformas que conforman voz son las Cisco 1751-V, 1760-V

La Cisco 1751-V está diseñada para sobre mesa mientras que la 1760 y 1760-V están montadas en un rack de 19 pulgadas. La extensión V indican que las

plataformas han sido ajustables con las memoria apropiada, imagen IOS y módulos DSP (Procesador de señal digital, Digital Signal Processor) para soportar voz.

Estas plataformas pueden completarse con tarjetas WIC (Tarjetas de interfaz de voz, Voice interface Cards) para soportar un amplio rango de aplicaciones. Las WIC ofrecen conectividad WAN como DSL de banda ancha, RDSI, líneas alquiladas y frame Relay, mientras que las VIC proporcionan conectividad PSTN como PRI (Interfaz de acceso principal, Primary Rate Interface).
T1 o E1 BRI (Interfaz de acceso básico, Basic Rate Interface) o FXO (oficina de intercambio remota, Foreign Exchange Office), y conectividad del lado de la estación usando FXS (Estación de intercambio remota, Station Exchange Office).

Las series Cisco 1700 soportan, entre otras, estas características:

- VoIP (Voz sobre IP, Voice over IP).
- Enrutamineto de alto rendimiento con QoS.
- Enrutamiento entre VLANs.
- Acceso VPN con opciones de firewall.

SERIES CISCO 2600XM Y PLATAFORMAS 2691. Las series Cisco 2600XM y los routers de la serie 2691 son plataformas montadas en rocks de 19 pulgadas que están dirigidas a empresas pequeñas o medianas y oficinas troncales. El catálogo incluye las plataformas Cisco 2611XM, 2621XM, 2651XM y 2691. Al igual que las series Cisco 1700, soportan las ranuras WIC y VIC.

Además, las Cisco 2600XM incluyen ranuras NM (modulo de red, Network Module) y AIM (Módulo de integración avanzado, Advanced Integration Module). El factor de forma NM es muy flexible, permitiendo un amplio rango de aplicaciones que van desde el correo de voz Cisco UE y AA al trunking PSTN de alta densidad y conmutación LAN. A diferencia de las WIC, VIC y NM, las AIM se instalan en la placa base del router. Este factor de forma soporta seguridad y aplicaciones de voz adicionales como correo de voz y DSP. La plataforma Cisco 2691 dispone de dos ranuras AIM, a diferencia de la 2600XM que sólo tiene una.

Las series Cisco 2600XM y 2691 soportan, entre otras, estas características:

- Integración multiservicio de voz y datos.
- Acceso VPN con opciones de firewall y cifrado.
- Servicios de acceso de marcación analógica.
- Enrutamiento con administración de banda ancha.
- Enrutamiento entre VLAN.
- Acceso DSL de alta velocidad.
- Integración de conmutación de baja densidad.

ROUTERS DE LA SERIE CISCO 2800. Estos routers incluyen las plataformas 2801, 2811, 2821, y 2851 y están dirigidos a empresas pequeñas o medianas y a oficinas troncales. Han sido diseñados para incluir voz, datos y seguridad en una WAN de alta velocidad para enlaces T1 o D2 sencillos o múltiples. Esto significa que

en lugar de ofrecer servicios añadiendo tarjetas a los routers, los Cisco 2800 ya integran esos servicios directamente en le chasis de la plataforma.

Los Cisco 2811, 2821 y 2851 disponen de ranuras HWIC (WIC de alta velocidad, High-speed WIC), VIC, NM y AIM, mientras que la 2801 soporta las mismas excepto la NM. Todas estas plataformas disponen de ranuras en su placa base para albergar tarjetas DSP.
Estas series soportan 4 variantes del factor de forma NM diferentes (módulo de red mejorado y ampliado de ancho doble) para incrementar la capacidad y un potencial futuro es crecimiento.
Las plataformas Cisco 2821 y 2851 también soportan un factor de forma EVM (Módulo de extensión de voz, Extensión Voice Module) de alta densidad que ofrece hasta 24 puertos de conexión analógica u 8 puertos (16 canales) de conectividad BRI. También exhibe un acelerador de seguridad hardware en la placa base que soporta el algoritmo de cifrado AES.

PLATAFORMAS 3700. Los routers de las series Cisco 3700 son los demás elevados prestaciones y cuentan con servicios de alta calidad como enrutamiento de alto rendimiento, conmutación de baja densidad integrada, seguridad, voz, telefonía IP, correo de voz y contenido de red. Estos servicios se ofrecen mediante ranuras WIC, VIC, NM y AIM. Estas series incluyen las plataformas 3725 y 3745.

La Cisco 3725 soporta dos ranuras de módulo de red, mientras la Cisco 3745 incluye cuatro. Además, la anchura de estas ranuras puede ajustarse para soportar servicios de alta densidad. Por ejemplo, las opciones EtherSwitch integradas incluyen un puerto NM 16 y otro 36, versión HDSM (Módulo de servicio de alta densidad, High-Density Service Module). E l puerto HDSM 16 utilizando la capacidad extra del factor de forma de la internas de módulo de red más ancha.

SERIES CISCO 3800. Las series Cisco 3800, similares a las 2800, son la última generación de routers de acceso y están diseñadas para servicios integrados. Las aplicaciones de datos, voz y seguridad están incrustadas en la placa base del router. Esto libera espacio y permite que las empresas se beneficien de las nuevas ranuras de alta velocidad, como HWIC y NME (Módulo de red mejorado, Network Module Enhanced), para servicios adicionales, interfaces y densidades. También se soportan las ranuras VIC, NM y AIM, así como las EVM. Los Cisco 3800 soportan además la aceleración hardware VPN.

Las series Cisco 3800 incluyen las plataformas 3825 y 3845. La primera soporta dos ranuras de módulo de red, mientras la segunda soporta cuatro.

Las series Cisco 3800 y 2800 mejoran sensiblemente el rendimiento y la integración del Cisco 1700, 2600 y 3700. Presentan mejoras en su arquitectura como características de seguridad en bebidas, DSPs en placa, gran cantidad de nuevos interfaces y un incremento de densidad de servicio. Por ejemplo, en lugar de usar un modulo de red NM-HDV2 para el acceso PSTN T1 o E1, ahora se puede utilizar una tarjeta de interfaz WAN o de voz T1 o E1 (VWIC) junto con los módulos DSP integrados en la placa del router (PVDM2). Esto libera las ranuras del módulo de red para otras aplicaciones como correo de voz y distribución de contenido.

CONSTRUCCIÓN DE UNA RED CISCO IPC EXPRESS. Express puede ser un excelente sistema de comunicaciones de voz y datos para su empresa y cómo sus opciones pueden adaptarse a sus necesidades. También ofrece algo de información acerca de las plataformas router, las licencias y los componentes que incluyen Cisco IPC Espress. Este capitulo trata del aspecto que debería tener su red, o dicho de formas más familiar, qué modelos de implantación es preciso considerar cuando se construye una red que contiene uno o más sitios con Cisco IPC Express.

Si usted es propietario de una pequeña empresa que opera en un único sitio, su red será igual se simple, sólo que una pequeña porción de información será la que se le aplique. En el otro extremo está el caso de que su negocio conste de muchos locales, o que trabaje para una firma que disponga de una red backbone empresarial, y esté considerando las instalaciones de Cisco IPC Espress en algunos, o en todos, los sitios troncales. Si éste es su caso, encontrará en este capitulo información muy útil acerca de la implantación de la red cuando se conecte Cisco IPC Express a su red actual. Por último, si es un SP (Proveedor de servicios, Service Provider) que está considerando ofrecer a sus clientes Cisco IPC Express como proveedor o CPE (Equipo terminal del abanado, Customer Premises Equipment), su red tiene más consideraciones a tener en cuenta.

4.34.- PANORÁMICA GENERAL DE LA IMPLANTACIÓN DE UNA RED TELEFONÍCA IP.

Antes de entrar en detalles concretos sobre Cisco IPC Express, se debe contar con una serie de conceptos básicos sobre las redes de telefonía IP y sus características propias, que serán los que le permitan saber cuál de todos los posibles modelos es el que mejor se ajusta a sus necesidades. Este conocimiento es imprescindible ya que las redes Cisco IPC Express siguen las mismas arquitecturas y premisas generales.

También presentan un pequeño subconjunto del amplio lienzo de opciones de telefonía IP entre las que pueden elegir para su negocio u oficina troncal. Otra razón importante para comprender las redes generales de telefonía IP es que se pueden mezclar y emparejar sistemas de diferentes tipos en la misma red. Si ya está familiarizado con estas arquitecturas puede saltarse la introducción y entrar en los modelos de implantación de Cisco IPC Express tratados en la siguiente sección.

El cerebro de una red de telefonía es el componente de control, o procesamiento, de llamada. Este componente puede estar colocado en cualquier lugar de la red en una o varias ubicaciones. Se encarga de ofrecer diferentes opciones de llamada a los teléfonos como el tono de marcado, la interpretación de los dígitos para implementar un plan de marcado y el establecimiento y finalización de las llamadas (o, de manera más técnica, un speech path o flujo de medios desde el emisor al receptor de esa llamada). El control de llamada también administra otras series de características suplementarias como la retención de llamadas, la transferencia, la conferencia, la MOH, el tono de espera de llamada, etc.

Cuando se está considerando dónde y cómo ofrecer el procesamiento de llamadas a los usuarios y los teléfonos, las redes de telefonía IP pueden clasificarse, en sentido amplio, en los siguientes tipos. Cada uno de ellos retrata con detalle en posteriores secciones:

- Red de sitio único o independiente (standalone).
- Red centralizada.
- Red distribuida.
- Red hibrida.

RED DE SITIO ÚNICO. Este tipo de redes se dan en áreas en las que todos los empleados están localizados en un único sitio, tal como puede verse en la figura. Por definición, este tipo de oficinas o redes son predominantemente de pequeño tamaño, con frecuencia con menos de 30 personas aunque, en ocasiones excepcionales, pueden llegar hasta las 100 ó 150. Una empresa más grande que ésta suele tener múltiples zonas geográficas.

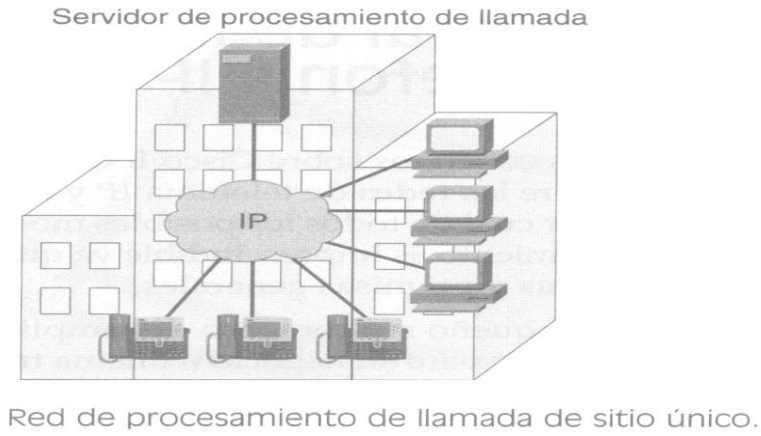


Fig.24.-Red de procedimiento de llamada de sitio único

En un despliegue tipo standalone, cada equipamiento del sitio almacena una instancia única del componente de procesamiento de llamada. En casos raros, y por motivos de redundancia, es posible que un sitio independiente implemente dos instancias de este componente. Sin embargo, esto raramente se emplea, ya que su coste es excesivo para un sitio pequeño. El disponer de uno o de dos teléfonos conectados directamente a la PSTN (Red Telefónica Conmutada Pública) (o a través de un puerto power failover del router) suele ofrecer u mecanismo de backup en el caso de que la redundancia sea algo completamente indispensable en su empresa.

RED CENTRALIZADA. En un negocio con múltiples localizaciones geográficas, se da más el caso de un sitio más grande, o que este más centrado, que el caso de una cierta cantidad de sitios más pequeños y remotos. En una topología de red centralizada, como la que puede verse en la figura, el componente de procesamiento de llamada suele estar centrado en su punto central o más grande, que con frecuencia es la central de la empresa. Este componente ofrece servicio a todos los teléfonos de los empleados de todos los sitios a través de la red que existe entre ellos.

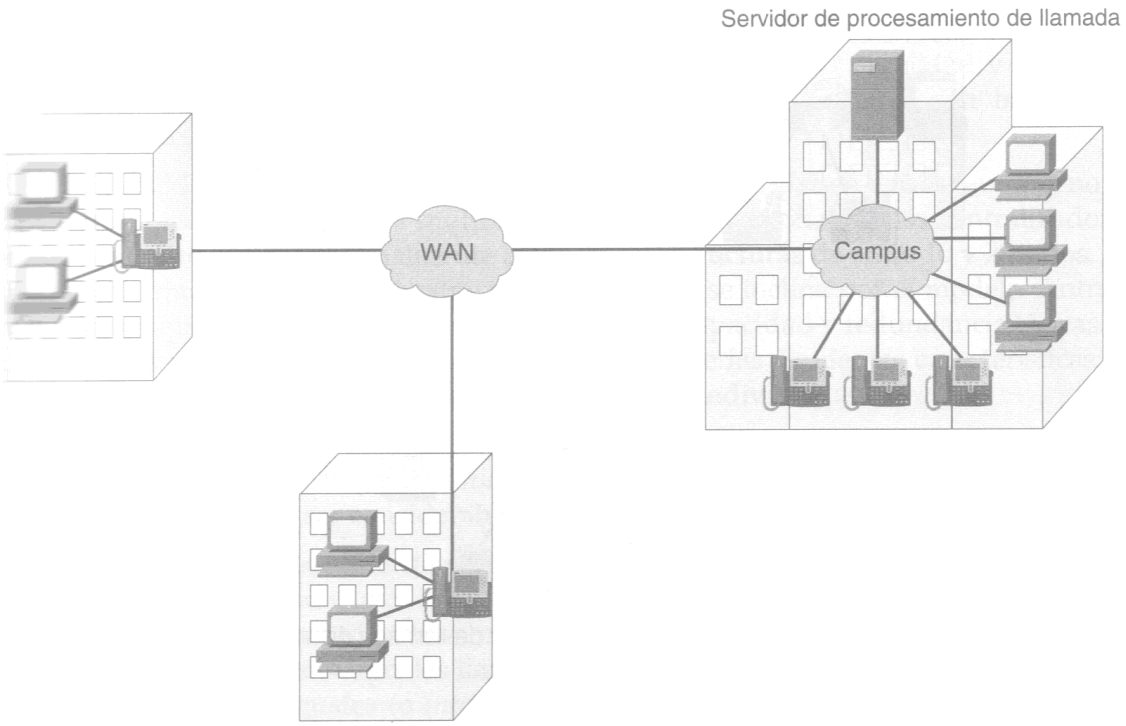


Fig.26.-Red de procedimiento de llamada centralizada.

En un esquema centralizado, uno de los sitios almacena una única instancia del componente de procesamiento de llamada, y el resto de sitios se conectan a él a través de la red IP existente entre ellos. Las llamadas se efectúan mediante *messaging* IP entre los dispositivos remotos (los telefónicos IP y las tróncales PSTN) y el componente central de procesamiento de llamadas.

Por razones de redundancia, las redes centralizadas pueden incluir múltiples instancias de este componente o, en el caso de redes de gran tamaño, para desviar la capacidad de llamadas y balancear la carga. En este modelo centralizado, estos componentes siempre están residentes en la sede central.

REDES DISTRIBUIDAS. En una red con varias localizaciones geográficas, es posible que cada sitio tenga la importancia que otros, lo que obliga a que la topología de la red esté duplicada. En estos entornos, cada sitio dispone de un servidor de procesamiento de llamadas para la totalidad de empleados (teléfonos IP) de este sitio.

Por lo tanto, una instalación distribuida consta de múltiples instancias del componente de procesamiento de llamada (uno en cada sitio) y cada uno de ellos reside en su propio sitio. Las llamadas entre cada ubicación se lleva a cabo mediante messaging IP entre iguales entre los dos componentes implicados en dicha llamada.
El tipo de arquitectura de red redundancia implícita, ya que cada sitio dispone de un componente de procesamiento de llamada. Una interrupción en la red o el servidor del Sitio A no afecta a las llamadas efectuadas en el sitio B. El modelo distribuido

también lleva implícita la escalabilidad en la capacidad de las llamadas y el balanceo de carga, porque cada sitio incorporado a la red dispone de su propia capacidad de procesamiento de llamadas. Estas son algunas de las ventajas de la arquitectura de red distribuida.

RED HÍBRIDA. La realidad de la mayoría de redes multisitio imposibilita que sea un modelo totalmente centralizado o distribuido. Por el contrario, muchas redes son un híbrido de ambos métodos. Una red que da soporte a muchos sitios suele contener varias localizaciones de gran tamaño en las que existe un número suficiente de empleados como para autorizar el uso de servidores de aplicación en campus dedicados. Una red de gran extensión suele contar con un importante número de sitios remotos que no son lo suficientemente grandes como para invertir una fuerte suma de dinero en equipos y administración.

Las restricciones de fiabilidad y disponibilidad también hacen que una red netamente centralizada no sea una elección muy acertada, ya que el fallo del único componente de procesamiento de llamada significa la caída completa de la red. Un pequeño número de servidores de procesamiento de llamada repartidos por los enclaves fundamentales ofrece una fiabilidad y cobertura mucho mayor en redes grandes. Además, estos pocos servidores son baratos de implantar y mantener.

La duplicación del componente de procesamiento de llamadas en varios sitios otorga a estas redes multisitio con aspectos de los modelos centralizados y distribuidos. Esto se hace especialmente evidente en estructuras de entre 10 y 20 sitios. En este caso, el atractivo de la administración centralizada se inclina por el modelo centralizado, a la vez que se consiguen las consideraciones de capacidad y redundancia típicas de un modelo distribuido. Este tipo de red híbrida incluye las siguientes características de cada uno de los modelos de procesamiento de llamada individual:

- Centralizado. Los sitios remotos obtienen los servicios de procesamiento de llamada a través de la red de otro *hub* centralizado. El número de sitios remotos en una red grande puede ser considerable (entre 100 y 500 sitios por *hub* centralizado).
- Distribuido. Varios sitios disponen de servidores de procesamiento de llamada (y, con frecuencia, cada uno de ellos dispone de una configuración redundante, o cluster). Estos elementos actúan como hubs para el resto de la red usando un diseño centralizado. Sin embargo, las llamadas realizadas entre los hubs representan comunicaciones entre iguales (o intercluster) entre el componente de procesamiento de llamadas distribuido. El número de sitios hub suele ser pequeño, de 5 a 20, incluso en redes grandes de más de 1000 sitios.

COMPARATIVA DE LOS SISTEMAS DE TELEFONÍA IP DE CISCO.

En una pequeña oficina independiente, Cisco IPC Express en una excelente solución. En redes mayores que cuentan con múltiples sitios, la decisión de centralizar o distribuir el procesamiento de las llamadas es un factor clave en el diseño de una red de telefonía IP. Es también uno de los factores fundamentales que indica si Cisco IPC Express es lo más adecuado para cada sitio individual.

Generalmente, es preciso considerar los productos de telefonía IP Cisco para el componente de procesamiento de llamada en una red independiente o multisitio, o para una sección de una red:

- Cisco CallManager. Es un servidor basado en el procesador Intel capaza de gestionar un rango de teléfonos IP de entre 1000 a 7500. Aunque el ROI (Rendimiento de las inversiones, Return On Investment) individual varia, Cisco CallManager no suele ser una elección costosa en sitios de menos de 500 teléfonos, aproximadamente. Es posible implantar Cisco CallManager en un modelo centralizado, distribuido o híbrido.
- Cisco IPC Express. Es un componente de procesamiento de llamada integrado en Cisco IOS que reside conjuntamente en el *router* del sitio. Puede ofrecer servicios de telefonía IP a sitios que no consten de mas 240 teléfonos.

Considerando Cisco CallManager y Cisco IPC Express, la decisión del diseño de la red no solo debe quedar en un dilema “centralizado o distribuido”, sino que también es importante escoger el mejor producto para cada sitio.

REDES Cisco CallManager. Las empresas compuestas por cientos o miles de sitios han encontrado que la mejor solución es una red Cisco CallManager centralizada. En este caso, el termino centralizado se emplea en un contexto menos rígido que en las secciones anteriores, y significa que la mayoría de teléfonos y sitios extraen sus servicios de procesamiento de llamada de otro sitio mas amplio. Pero, inevitablemente, existen numerosos servidores Cisco CallManager distribuidos a lo largo de los puntos centrales de la red por lo que esta red es modelo híbrido.

En este tipo de redes, el correo de voz también suele estar centralizado y es ofrecido por servidores a gran escala que cuentan con cientos, o miles, de usuarios por servidor. Otras muchas aplicaciones, como el correo electrónico y las aplicaciones de empresa, también podrían estar localizadas en el mismo sitio y concentradas ene l mismo centro de datos. Por consiguiente, existe un recurso centralizado para la mayoría de sitios remotos de la red.

Ofrecer tanto el procesamiento de llamadas como los servicios de correo de voz de una forma centralizada obliga a disponer de los siguientes atributos de negocio y de red:

- Ancho de banda WAN suficiente para las llamadas efectuadas desde los sitios remotos a la central, lugar en el que están los servidores.

- Una WAN diseñada con QoS en todas las localizaciones remotas.
- Disponibilidad de la red (*uptime*) que cumpla las expectativas de servicio telefónico de los usuarios remotos.
- Un modelo de administración T1 central y profesionales sólidos.
- Una campaña institucional de presentación de la telefonía IP a todos, o la mayoría, de los sitios.
- Una red empresarial solidamente integrada tanto en términos tecnológicos como administrativos.

Aunque los puntos anteriores suelen estar presentes en la mayoría de redes de empresas grandes, las de negocios de pequeño y mediano tamaño no suelen contar con ellos.

REDES Cisco IPC Express. Las empresas a las que un sistema Cisco IPC Express podría venirle bien son aquéllas que cumplen algunos, o todos, de los siguientes puntos:

- Empresa independiente de un solo sitio.
- Está abastecida por una WAN, aunque no suele disponer del suficiente ancho de banda como para transportar llamadas entre dos sitios, o existen otras razones de logística para no utilizar la WAN para estos cometidos.
- Aun existiendo una WAN, no se ha implementado QoS en la red y él hacerlo podría suponer un coste excesivo, o la WAN está compuesta de segmentos de Internet que, intrínsecamente, no ofrecen garantías QoS.
- Un modelo de administración autónomo para localizaciones remotas, o una red empresarial pobremente integrada, ambos en términos de tecnología y administración.
- No existe una organización T1 central o experimentada.
- Los patrones de llamada predominantes de la empresa entre localizaciones remotas y sus clientes PSTN locales, con muy volumen entre las sucursales.

Es posible vincular varios sitios Cisco IPC Express a través de una infraestructura IP y apalancar esa red con llamadas VoIP (Voz sobre IP). En este caso, las consideraciones con Cisco CallMAnager y Cisco IPC Express se vinculan a lo siguiente:

- La tecnología y características disponibles de cada producto. Por ejemplo, Cisco IPC Express puede realizar *paging* mientras que Cisco CallManager no, por lo que si esta característica es necesaria, hay que decidirse por este modelo.
- La estrategia de presentación de VoIP puede comenzar con tres o cinco sitios conectados para, más tarde, migrar toda la red a una solución Cisco CallManager centralizada.
- No existe un sitio central claro capaz de albergar el sistema de procesamiento de llamada con un cierto grado de fiabilidad, por lo que el procesamiento local en cada sitio está más en la línea del negocio, lo que suele ocurrir con frecuencia en el segmento del comercio.
- Sus sitios remotos tienen una considerablemente autonomía, como por ejemplo una franquicia. Por ello, prefieren poner en marcha y administrar sus

propios teléfonos IP, sistemas de procesamiento de llamada y servicios de correo y voz.

REDES HÍBRIDAS CISCO CALLMANAGER Y CISCO IPC EXPRESS.

Aunque pueda parecerlo, la decisión de implantar en una red solo Cisco IPC Express o solo Cisco CallManager no está del todo clara. Un diseño híbrido con un Cisco CallManager centralizado dando servicio a varios sitios y un Cisco IPC Express para otras localizaciones puede tener sentido para ciertas redes.

Son varios los atributos que pueden sufrir que una metodología híbrida seria una buena solución:

- Una buena disposición de la WAN.
- Una estrategia de presentación de la telefonía IP.
- Prácticas de negocio diversificadas.

Buena disposición de la WAN. Algunos segmentos de la WAN disponen de ancho de banda y QoS para el tráfico de voz, pero de otros sitios no. Estas ubicaciones podrían conectarse con una tecnología en la que no tendría demasiado sentido económico aumentar al ancho de banda o diseñar el acceso a la WAN para ofrecer QoS. Y también podría darse el caso de que estas conexiones no serían lo suficientemente rentables como para combinar la conectividad o ancho de banda de la WAN.

Estrategia de presentación de la telefonía IP. Se podría plantear una situación en la que se desease iniciar un proyecto piloto de telefonía IP en algunos sitios con pocos usuarios, con vistas a una futura implantación de toda la red en una estrategia de varios años y varias fases.

Dependiendo del número de usuarios del proyecto piloto, un Cisco CallManager podría ser demasiado caro o demasiado grande, por lo que un Cisco IPC Express es una opción atractiva para empezar. Todos los teléfonos, routers, switches, licencias y otros componentes de voz pueden reutilizarse una vez tomada la decisión de migrar todo el sistema a un Cisco CallManager centralizado.

Prácticas de negocio diversificadas. Ciertas empresas están constituidas de forma que algunos de sus sitios trabajan muy estrechamente entre sí y se encuentran bajo la administración de una organización T1. Otros sitios, y en función del tipo de negocio que manejen dentro de la empresa, pueden ser mucho mas autónomos y tener poco contacto con el resto de la organización. Por ello, la administración T1 puede ser cedida directamente a ellos.

Esta situación podría darse por la adquisición de una compañía con una filosofía de negocio distinta, una empresa de gran tamaño que separa ciertas partes del negocio para ser más autónomas o un negocio principal que franquicia sus agencias.

Comprender los modelos de implantación de Cisco IPC Express

Esta sección se centra con más detalle en los distintos tipos de implantaciones de redes Cisco IPC Express. Se da por sentado que alguno de los modelos tratados anteriormente se ajusta a las necesidades de su organización.

Aquí se tratarán tres modelos de implantación generales:

- Oficina independiente. Una empresa con un único sitio que consta de menos de 100 empleados.
- Empresa con varios sitios. Una oficina troncal o remota intercomunicada con otros sitios de la misma red.
- Servicios administrativos por un SP. Puede ser de alguna de las dos categorías anteriores. En lugar de comprar y administrar el equipo, se paga una cantidad periódica a un SP local, el cual dispone de los equipos y alberga los servicios, tanto los de voz como los de datos.

Oficina independiente. Este modelo se adapta a ese vasto número de pequeñas compañías de un solo sitio que están desparramadas por todo el mundo y que tienen menos de 100 empleados, algunos ejemplos son:

- Una clínica dental.
- Una pequeña clínica sanitaria
- Oficinas de servicios profesionales como arquitectos, abogados o decoradores de interiores.

Este tipo de negocios no cuente con una estructura T1, y toda la plantilla se encarga de llevar a cabo los procesos habituales. Los servicios de datos y voz que soportan estos negocios están albergados por un SP local o instalados y mantenidos por una VAR (Valor añadido de reventa) local o un SI (Integrador de sistemas)

La telefonía IP puede ser tan positiva para ese tipo de negocios como es para expresas con una experta plantilla TI. Los servicios de voz d este tipo de compañías suelen estar proporcionados por servicios centrex o por un sistema clave instalado por un VAR o SI. El servicio de datos lo proporcionó el ISP (Proveedor de servicio a Internet) local, el cual colocó algún tipo de CPE en las oficinas que administra desde un punto local central.

Para cualquier sitio, excepto para los muy pequeños a los que cuentan con uno o dos empleados, el CPE debería incluir un router y servicios de seguridad básicos como un firewall.

Las siguientes secciones exploran diferentes aspectos de la red de una oficina independiente, incluyendo su arquitectura, sus aplicaciones, su administración y sus servicios de seguridad.

ARQUITECTURA DE LA RED. Cisco IPC Express es una excelente elección para una oficina independiente. En el mundo antes de la telefonía IP, este tipo de oficina debía contar con un router propio para los servicios de datos y un sistema clave aparte, o centrex, par los de voz. Ahora, el router puede ampliarse para ofrecer ambos servicios. La administración puede llevarse a cabo del mismo modo que

antes, bien por un ISP o por un VAR o un SI. Además, tanto el negocio como el SP pueden ahorrar costes, espacio y administración.

Sólo el ahorro en cableado de la oficina puede ser lo suficiente para invertir en Cisco IPC Express. Ya que tanto los teléfonos como los computadores están basados en Ethernet, sólo es necesario cableado de este tipo. Por otro lado, cada empleado solo precisa de un jack Ethernet. Los equipos informativos pueden conectarse a la parte trasera del teléfono, lo que permite el uso de tecnología VLAN (LAN virtual) para conseguir una separación virtual (y, por consiguiente, segura) de voz y de datos. También puede instalarse en esta infraestructura aplicaciones IP mejoradas de servicio al cliente, como servicios XML y características de productividad.

La figura muestra el aspecto que podría tener una oficina como ésta. La figura tiene los siguientes componentes:

1.- Escritorio del empleado. Los teléfonos Cisco 7960 IP son ofrecidos a los empleados que trabajan en un escritorio con un computador. El PC se conecta a través del teléfono fono al switch Ethernet. También se une al switch LAN mediante in sencillo cable Ethernet para suministrar energía a los teléfonos. En la figura, el switch LAN es un componente aparte, aunque puede integrarse en el chasis del router en oficinas que requieran 50, o menos, conexiones LAN. La posibilidad de conectar un computador a través del teléfono reduce sustancialmente el número global de puertos switch necesarios en la oficina. Sin embargo, esto podría obligar a actualizar el switch LAN existente para que pueda suministrar potencia a los teléfonos IP.

2.- La conexión a Internet la proporción una DSL o algún tipo de enlace similar con el ISP local, el cual podría albergar también los servicios de correo electrónico de la empresa. En oficinas mayores, puede que una DSL no ofrezca todo el ancho de banda necesario. En estos casos, la conexión a Internet puede obtenerse mediante el alquiler de líneas T1/E1 fraccionadas, o incluso fraccionando varias líneas DSL o BRI (Interfaz de acceso Básico).

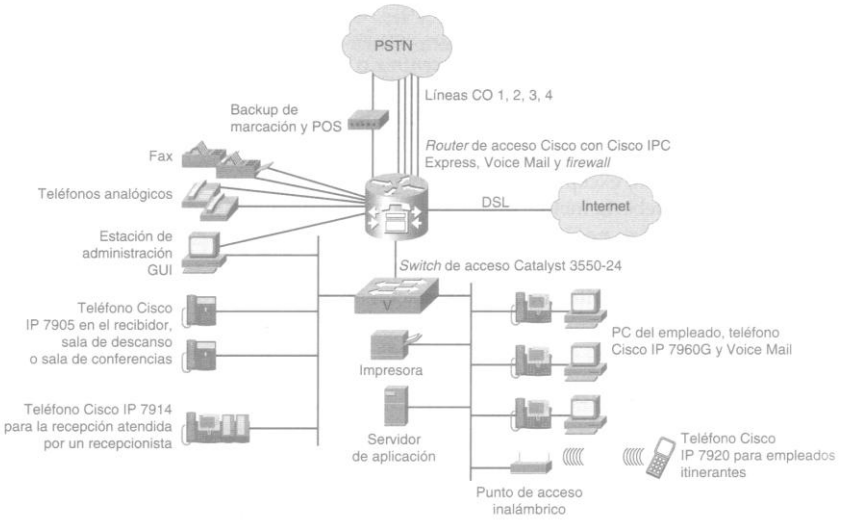


Fig.26.-Topología de una red independiente

3.- Troncales PSTN. Las pequeñas empresas suelen preferir la operativa de los sistemas clave a los que ya están familiarizados. En estos sistemas existen líneas PSTN individuales asociados a los botones de los teléfonos. Cada uno de ellos está identificado como Línea1, Línea2, Línea3, etc. Hasta completar el total de líneas de la oficina central PSTN (esta disposición recibe el nombre de configuración línea compartida). Estas líneas PSTN son conexiones FXO (Oficina de intercambio remota) analógicas con la CO (Oficina central). Cada línea transporta una única llamada telefónica entrante o saliente. El identificador de la persona que llama se envía en este tipo de conexiones, pero la operación DID (Marcación Directa Interna) no. Una variación de esta oferta PSTN ofrece el funcionamiento DID; esto se conoce técnicamente como servicio DID analógico, que puede tener un coste diferente al del servicio FXO plano.

4.- Recepción atendida. Muchas pequeñas empresas que cuentan con una cantidad media de empleados o una considerable relación con los clientes (como una clínica sanitaria) prefieren que una recepcionista responda a las llamadas. Aunque estas empresas podrían utilizar una AA (Operadora automática) para prestar servicio fuera de las horas de oficina, lo norma es que prefieran la interacción personal con los clientes durante las horas de trabajo.

EMPRESA. Estación de administración. Es una aplicación de GUI web que se encarga de los movimientos diarios, la incorporación y modificación de los cambios en la configuración del sistema.

Otros servicios de voz. Cualquier tipo de negocio dispone de uno, o varios, faxes, además de contar un pequeño número de teléfonos analógicos para tareas varias, como la conectividad PSTN backup de emergencia para el descanso de producirse un corte en el suministro energético del edificio.

Los teléfonos IP de bajo coste, como el Cisco 7902 ó el 7905, son los que se encuentran diseminados a lo largo de la oficina en las salas de descanso, las consultas de las clínicas sanitarias, recepciones y, quizás, en las salas de conferencia.

Estos terminales suelen se teléfonos de líneas única que no suelen utilizarse para recibir llamadas de la PSTN (tampoco disponen de puertos Ethernet para PC), sino que se emplean para realizar llamadas dentro de la oficina o al exterior. Por tanto, los teléfonos IP participan en los sistemas de megafonía, el paging y en los servicios de display más utilizados en el entorno de una pequeña oficina.

El teléfono inalámbrico Cisco 7920 también puede ser una herramienta para mejorar la productividad de aquellos empleados que tienen que moverse para las dependencias pero que deben estar siempre localizables, como los supervisores de planta, un encargado de almacén o el director de una sucursal bancaria.

APLICACIONES. En cierto tipo de negocios, el correo de voz es esencial. En estudios de arquitectura y despachos de abogados, el contacto personal con el cliente es fundamental para el manejo del negocio. En otro tipo de empresas, como restaurantes o pequeños almacenes, este tipo de aplicación no es tan necesario.

Una pequeña compañía no suele utilizar una aplicación AA durante las horas de trabajo; el cliente prefiere el contacto personal con la recepcionista. A pesar de todo, la AA sigue siendo un sistema esencial fuera del horario de oficina para ofrecer información acerca del horario, la dirección de la sede y, quizá, para informar del cierre temporal del despacho por causas inesperadas.

Las aplicaciones XML específicas del segmento industrial pueden ajustarse a cada negocio para mejorar la productividad del mismo o mejorar la atención al cliente, Por ejemplo, una oficina de correduría de bolsa puede contar un *ticker* de las cotizaciones funcionando constantemente en la pantalla del teléfono. Un hotel podría contar con una aplicación que mostrase el estado de las habitaciones. Dicha aplicación refleja la disponibilidad de la misma en el momento en que el servicio de limpieza la dejase preparada para el siguiente cliente.

ADMINISTRACIÓN. Con la última tecnología GUI web, una persona sin conocimientos técnicos puede modificar parámetro del sistema sin necesidad del VAR o SI que lo instalo. Como ejemplos de este tipo de modificaciones se pueden citar los siguientes:

- Añadir buzones de voz.
- Cambiar la locución de los nombres de los empleados.
- Añadir o cambiar una extensión dentro de la oficina.
- Incorporar una extensión y un buzón de voz para un nuevo empleado.

Sin embargo, la instalación del sistema, la configuración inicial, las actualizaciones de software y la activación de nuevos servicios son tareas que debe llevar a cabo el SP, o bien el SI o el VAR al que se adquirió o alquiló el sistema. Si se sufre cualquier problema, astas organizaciones serán las responsables de aislarlo y trabajar junto con el vendedor del sistema para la correcta solución del mismo.

SEGURIDAD. Cualquier red, y especial las conectadas a Internet, precisan de una serie de medidas de seguridad para proteger el sistema, las aplicaciones y la propia red de cualquier acceso no autorizado. Como mínimo, es preciso utilizar un firewall. También precisará de varias ACL (Lista de control de acceso, Access Control List) para limitar el acceso a las direcciones IP y los puertos del equipamiento conectado a Internet (routers) y los sistemas que están detrás de ellos (teléfonos IP, servidores de aplicaciones o PCs). La protección contra los virus, la detección de intrusiones y el NAC (Control de acceso a la red, Network Access Control) de cliente también suelen ser necesarios.

Es improbable que los empleados de una pequeña oficina estén involucrados directamente n la definición o el establecimiento de las medidas de seguridad de la oficina. Por lo general, el SP o el VAR/SI que proporcione el sistema suele ser el encargado de implantar los mecanismos de seguridad durante la instalación y configuración inicial del mismo.

EMPRESA O NEGOCIO MULTISITIO. Este modelo puede ser una buena elección para la red de una empresa de cualquier tamaño. En general, Cisco IPC Express es

una mejor solución para los sistemas de nivel bajo (una red con un número pequeño de sitios y menos de 200 empleados por cada uno). Cuanto mayor es la red (es decir, más sitios y empleados tiene), más claro parece que la mejor solución a adoptar es un Cisco CallManager centralizado.

Como ya se comentó en la sección anterior “Redes Cisco IPC Express”, muchas de estas redes multisitio un Cisco CallManager centralizado (para el procesamiento de llamada) y un Cisco Unity (para el messaging unificado basado en servidor). Pero Cisco IPC Express todavía sigue siendo una buena elección para pequeñas compañías, o para ciertos (o todos) los sitios de empresas mayores, por las razones que se enumeraron anteriormente.

Esta sección considera dos tipos de redes en el modelo de empresa multisitio:

Empresa pequeña. Por lo general, es la que cuenta con un número pequeño de sitios (por ejemplo, con menos de diez) interconectados todos ellos a través de sistemas Cisco IPC Express.

Empresa híbrida. Habitualmente, está compuesta por una elevada cantidad de sitios de los que sólo un pequeño número de ellos utiliza Cisco Express. El resto continua usando los sistemas clave o PBX (Conmutador telefónico privado, Private Branch Exchange).

Cuanto mayor sea la empresa, más estructura y organización TI hace falta. Por consiguiente, estas compañías suelen contar con personal de este tipo en plantilla. También administran sus propias redes, o las rentan a los SP que están especializados en dar servicio a empresas de este tipo.

Por muchas razones, la telefonía IP en empresas con muchos sitios puede ser un tema a considerar. Por ejemplo, supone un ahorro en el cableado y en los cargos de las llamadas internacionales, las aplicaciones de las disposiciones mejoran la productividad y la propia infraestructura de la red hace que se tenga que administrar mucho menos equipo. Otra forma de ahorrar es que el sistema ofrece una plantilla común para el equipamiento y la topología de la red que puede emplearse en un gran número de localizaciones remotas, todas ellas con una configuración idéntica (un ejemplo puede darse en las tiendas de una cadenas de almacenes, en las que la panadería siempre está en la extensión 5000 mientras que la carnicería puede encontrarse en la 4000)

La media de oficinas troncales de la red de una empresa siempre cuenta con un router entre sus necesidades. La incorporación de Cisco IPC Express sólo requiere que se actualice el software (y quizá, la memoria), puede que la incorporación de algunos componentes hardware (como tarjetas de interfaz de voz para troncales PSTN) y la implantación de teléfonos IP.

Siempre existe una excepción en cada generalización, y esto es especialmente ciento en los modelos de implantación de una red. Aunque las empresas grandes siempre tienden más hacia un modelo híbrido que hacia un Cisco CallManager Centralizado, otras muchas, con cientos de localizaciones, utilizan Cisco IPC

Express en cada sitio, los cuales interconectan a través de sus propias redes. Esto suele darse con bastante frecuencia en el comercio al por menor, ya que este modelo cumple a la perfección con las expectativas del negocio.

LA PEQUEÑA EMPRESA. En el grupo de pequeñas empresas pueden incluirse las siguientes:

Una empresa de préstamos local, o un pequeño banco, con algunas sucursales en un área geográfica restringida.
Una pequeña cadena de almacenes que cuente con algunas tiendas en una ciudad o estado.
Una cadena de clínicas sanitarias pertenecientes a un hospital o a una HMO (Organización de Atención Médica Administrada, Health Maintenance Organization).

Las siguientes secciones se centran con más detalle en la red empresarial típica de este tipo de negocios, incluyendo su arquitectura, aplicaciones, administración y sistemas de seguridad.

ARQUITECTURA DE LA RED. Cisco IPC Express es una excelente elección para pequeños negocios que cuenten con un pequeño número de oficinas (diez, o menos). El punto en el que un Cisco Call Manager centralizado empieza a tener sentido depende de:

- El negocio individual.
- Su estilo de administración.
- La buena disposición.
- La buena disposición QoS de la red existente entre los sitios.
- El coste de la conectividad entre los sitios.
- Lo junto, o separados, que trabajan dos sitios en una jornada laboral cualquiera.

En una empresa con un modelo de negocio en el que las sucursales estén muy poco relacionadas entre sí, podría bastar con interconectar esos sitios mediante Cisco IPC y PSTN para el acceso por voz. Un ejemplo de esto podría ser una cadena de restaurantes. En esencia, este tipo de red se ajusta al modelo standalone comentado en la sección anterior. Ya que los centros sólo se comunican entre sí mediante PSTN, no es preciso enlazarlos mediante VoIP y la topología de la red de cada localización se parecería al de una entidad standalone (desde una perspectiva de tráfico de voz).

El caso más interesante con el que nos podemos encontrar se da cuando una empresa con muchas oficinas decide que la implantación de la conectividad VoIP es ventajosa desde el punto de vista de ahorro de tarifas, o por motivos de administración.

La figura 27 muestra un ejemplo de topología de la red de una oficina troncal de la empresa. Esta representación ofrece una visión general de dicha oficina.

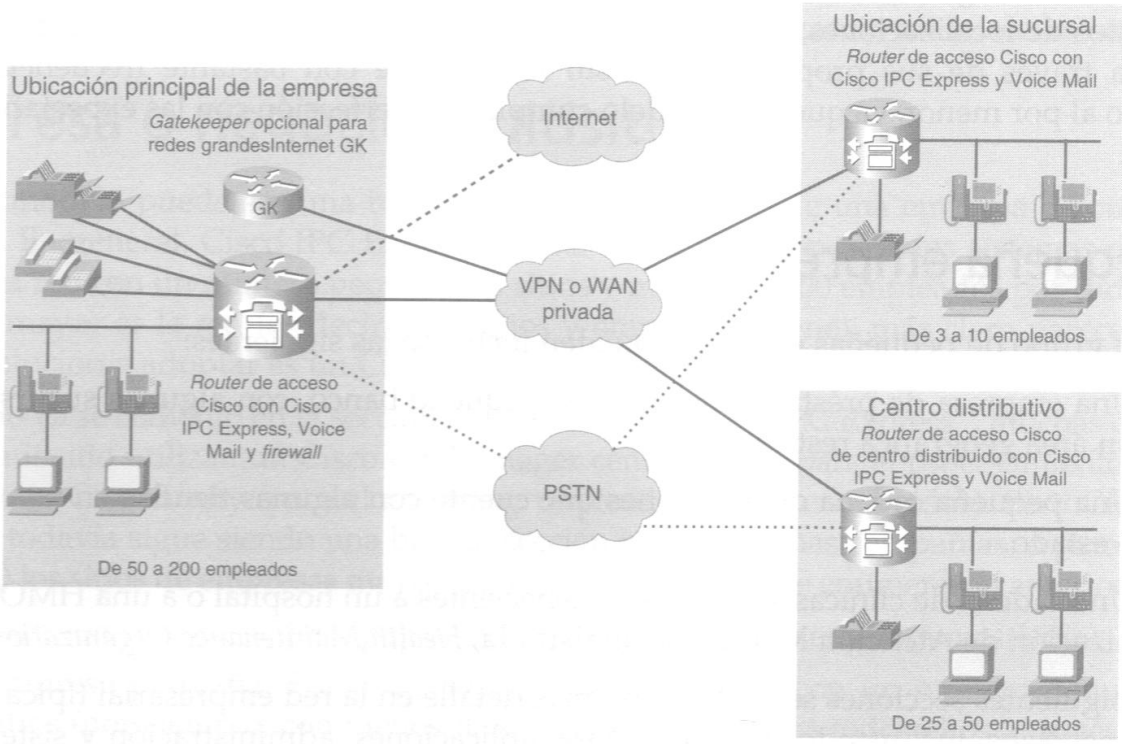


Fig.27.-Arquitectura de red Cisco IPC multisitio y distribuida.

Existen bastantes similitudes entre el esquema de la pequeña oficina troncal y la del modelo de sucursal independiente de sitio único mostrado anteriormente. Las siguientes son algunas de las nuevas consideraciones:

- Empleados de oficina. Dependiendo del tipo de negocio, el porcentaje de estos trabajadores varía. Un almacén, por ejemplo, cuenta con muchos menos que un banco o una compañía de seguros. Por tanto, existen empleados que, por su tipo de trabajo o por la ubicación en la que lo desempeñan, no cuenta con los teléfonos individuales o computadores, sino que utilizan recursos compartidos desplegados a tal efecto. Las llamadas personales se realizan desde cabinas públicas ubicadas en las salas de descanso, o desde un pequeño número de teléfonos repartidos en el espacio común de los trabajadores, a los cuales pueden acceder durante sus periodos de descanso.
- Conectividad WAN. La red desplegada entre los sitios suele ser algún tipo de WAN privada. También puede ser una VPN (red privada virtual, Virtual Private Network) que utilice internet como medio de transporte, aunque al no contar con Qos no es una buena elección para la distribución del tráfico VoIP.

- Una WAN compatible con VoIP es lo más correcto, ya sea ésta propiedad de la empresa o esté alquilada a un SP. En la parte superior del servicio de red podría emplearse una VPN. La conectividad de cada sitio depende de la localización geográfica del mismo y de sus necesidades de ancho de banda. Podría ser DSL, BRI, acceso T1/E1 fraccionado e, incluso, metro-Ehernet. Las oficinas más distantes podrían necesitar de una línea T1/E1 completa, o

enlazar varias DSL o líneas de acceso físico BRI para proporcionar un ancho de banda superior.

- La oferta norteamericana de acceso integrado, que engloba canales de voz y datos que comparten la misma T1 física, es una posibilidad muy atractiva para este tipo de oficina. La conexión de voz (PSTN) puede conseguirse a través de señalización en banda T1 (T1 CAS [Señalización de canal T1 asociado, T1 Channel Associated Singaling]) o mediante PRI fraccionado. La conexión de datos suele ser frame relay.

- La conectividad PSTN también depende del tamaño de la oficina y de su localización. Podrían ser conexiones de baja densidad analógicas (FXO o DID analógica) o BRI, o T1/E1 fraccionadas de alta densidad, quizá con un servicio PRI (Interfaz de acceso principal, Primary Rate Interface) fraccionado.

- El modelo de negocio y el tamaño de la oficina son los que dictan si dicha oficina utilizará una operativa de sistema clave (Línea 1, Línea 2, etc. En función de los botones de cada teléfono) u otra tipo PBX, con una sola extensión por teléfono y servicio DID desde el CO.

- Las oficinas más pequeñas suelen tender al uso del primer tipo de operativa, por que es el sistema de voz tradicional que tenían instalado antes de la implantación de un sistema de telefonía IP. En oficinas más grandes, se hace imposible tener un botón para cada troncal CO entrante. Estos sitios suelen ser mejores candidatos al servicio DID. Una persona, o un AA, reciben todas las llamadas y las redirigen al departamento o empleado correspondiente.

- Otros servicios de voz. Cuando unos cuantos sitios (cinco de menos) están interconectados, el plan de marcación on-net suele ser tan simple que puede implementarse en cada sitio. Sin embargo, este engranaje de sitios se va haciendo más difícil de administrar a medida que aumenta el número de éstos. Para este objetivo, se muestra un gatekeeper (GK) en el sitio principal de la figura 2.5. En empresas de diez o más localizaciones, lo mejor es centralizar la administración del plan de marcación. Para ello, un GK H.323 es lo mejor cuando se interconectan varios sitios con Cisco IPC Express. De esta forma, el plan de marcación se administra desde una sola localización y no está duplicada en cada sitio.

APLICACIONES. El coreo de voz y las aplicaciones AA fueron grandes impulsoras de la productividad cuando fueron presentadas hace ya una o dos décadas. Por ahora, son servicios esenciales en la mayoría de las empresas. Aunque una recepcionista sigue un factor fundamental en la interacción con el cliente y para acompañarlo a su destino, un sistema AA o IVR (Respuesta interactiva de voz, Interactive Voice Response) suplementario se hace indispensable a medida que el negocio crece. Las preguntas de los clientes que más se repiten siempre son las mismas y se refieren a balances de cuentas, direcciones y horario de las oficinas, encargo de formularios, resultados de pruebas médicas y otros servicios.

Las aplicaciones XML específicas del segmento industrial pueden ajustarse a las necesidades de cada una para aumentar la productividad o mejorar la relación con el cliente.

ADMINISTRACIÓN. Muy probablemente, al igual que ocurre con el GK de la localización principal, existe un sitio que es más amplio, o está más concentrado, que otro en la operativa de la empresa. Todos los sitios están administrados desde esta localización. Esta operación puede ser tan simple como disponer de un único servidor desde el que se acceda a las GUI de los sistemas Cisco IPC del resto de sitios, lo que permite disponer de herramientas de administración y monitorización más sofisticadas.

SEGURIDAD. Las medidas de seguridad son temas fundamentales para muchas empresas. Ya que muchos de los sitios individuales no están conectados directamente a internet, sino que lo hacen a algún SP o VPN de la empresa, se obtiene una cierta seguridad de los equipos del SP, los firewalls y sistemas de detección de intrusiones, sobre todo si alguno de los sitios está conectado directamente a internet o dispone de acceso a la red de la conexión WAN privada establecida entre los sitios.

CAPITULO 5 IMPLEMENTACIÓN DE TELEFONÍA IP SOBRE VPN.

5.1.- IMPLEMENTACIÓN DE TELEFONÍA IP SOBRE VPN.

Utilizar la tecnología actual es de gran importancia, ya que en realidad la tenemos a la mano y en muchas ocasiones desconocemos el potencial que se puede generar, dando aplicaciones importantes y especificas.

En la actualidad por distintas razones las empresas no tienen en su totalidad al personal laborable dentro de las mismas instalaciones, lo que ocasiona que tengamos información no actualizada y centralizada.

En el caso de ingeniería aplicada en campo y arquitectos residentes de obra, son partes importantes de una empresa los cuales utilizan y generan información actual, que es de gran importancia en la toma de decisiones, esta información puede ser desde planos, hasta listados de pedimento de material y/o cotizaciones. Con la aplicación de VPN´s de acceso remoto nosotros tendremos la información en tiempo real y compartir recursos de una oficina de manera segura, como lo es un servidor de almacenamiento en el cual cualquier persona autorizada, puede utilizar esta información actualizada.

Otro ejemplo son agentes de ventas, los cuales pueden estar en contacto con el stock, ya que la información se actualiza en un servidor de manera segura y en tiempo real. Evitando de esta manera conflictos por ventas duplicadas o por falta de mercancía.

5.2.- PLANTEAMIENTO DEL PROBLEMA.

En las instalaciones actuales de BIOGAMA donde desarrollaremos la solución se encuentra en las siguientes condiciones.
Para el servicio de voz cuentan actualmente con un conmutador multilíneas, soporta 3 líneas troncales y 8 extensiones analógicas respectivamente, los teléfonos con los que se cuentan son también analógicos.
Respecto al servicio de datos, se cuenta con acceso a Internet de 2 MB utilizado para tener comunicación vía correo con los clientes y para realizar compras de bases para licitaciones, entre otras cosas. La aplicación más crítica con la que se cuenta es el programa SAE de Aspel, el cual les ayuda para mantener su inventario al día y manejar toda la parte de pedidos, remisiones y facturación.

Realizamos un listado del equipo con el que cuentan y detallando de una manera conceptual su función en la red junto a un diagrama con la topología de su red.
(Ver en anexo A)

Equipos de comunicaciones:

- Router Linksys inalámbrico que recibe la conexión a Internet del proveedor de servicios Telmex y da el servicio inalámbrico para equipos portátiles como Laptops o PDA´s.

- Switch 3com de 16 puertos 10/100, este equipo no es administrable e interconecta todos los equipos de la red.
- Conmutador Panasonic multilíneas, 3 troncales y 8 extensiones
- Teléfonos Panasonic analógicos.

Cuentan con los servicios de firewall, administrados por el router Linksys, al inicio de sus operaciones este esquema era funcional, en estos momentos carecen de un equipo de seguridad dedicado para proveer los servicios de firewall, detección de intrusos o filtrado de contenidos, encontramos la debilidad de poder conocer todos los movimientos (facturación, pedidos, etc.) en tiempo real. Esta observación no es el objetivo del presente documento, solamente se hace referencia por ser una propuesta de la implementación.

Cuentan con servicios telefónicos analógicos, que ayudan a saber información que necesitan, pero no es de forma directa, a esto le agregamos el costo que es mantener a varias personas, con planes de telefonía celular para cubrir sus necesidades de comunicación con el sitio central.

Es importante mencionar que los clientes buscan a nuestros vendedores, para hacer un pedido o una consulta, si le marcan a su teléfono celular y no se tiene una comunicación al momento, se pueden tomar decisiones importantes, como generar una orden de compra de un producto que no se tiene, esto es con la finalidad de satisfacer la necesidad del cliente lo más rápido posible.

Como esta descrito en los párrafos anteriores, el problema medular es tener a las personas comunicadas no solamente en la parte de telefonía, también en las aplicaciones de datos que la empresa está utilizando, teniendo como resultado buenas decisiones o estrategias. Resumiendo lo anterior, se encuentran los siguientes problemas específicos:

1.- La información de los inventarios, pedidos, facturación en tiempo real, es una necesidad indispensable para la empresa para dar un mejor servicio a lo clientes y tener una administración interna optimizada.

2.- Altos costos en telefonía para mantener comunicada a las diferentes personas que integran la empresa, como vendedores, repartidores, administrativos, entre otras.

3.- Mantener la información segura sobre ambientes o redes no seguras.

4.- No contar con una comunicación eficiente entre las personas que integran la empresa.

5.3.- PROPUESTA DE SOLUCIÓN AL PROBLEMA.

La solución consiste en implementar por hardware, equipo adicional a su infraestructura de datos y utilizar su servicio que ya pagaba de Internet.

Por otra parte se requiere un software que consiste en 2 programas para PC, los cuales son libres (no tienen un costo) y tienen convivencia con la tecnología a configurar en el router. (Ver anexos A y B).

El equipo es un ROUTER CISCO 2801 donde se integraron 3 tarjetas: 1 WIC-ADSL, 1 FXS y 1 FXO, para configurar el router de la siguiente manera:

- La tecnología ADSL, es con la que obtendremos el internet, utilizando a nuestro proveedor de servicio.
- La tecnología de VPN (red privada virtual), logrando con esto enlaces seguros, entre la oficina y el personal móvil,
- VoIP, tecnología con la cual nos comunicaremos con todo el personal que compone la empresa siempre que se cuente con el recurso siguiente: una computadora personal o un teléfono Ip.

El software que se instalara en los equipos de cómputo portátiles es el VPN Client de cisco, con él realizaremos un enlace VPN de tipo acceso remoto.

El softphone, es el otro software a instalar mediante el cual realizáremos la comunicación de VoIP a través de la PC.

Con todo lo anterior resolveremos los problemas que se encontraron en la situación actual, la cual consistió en instalar una red que sea capaz de integrar los servicios de voz y datos, así como también recibir conexiones de Internet para poder tener comunicación telefónica sin necesidad de usar los servicios a celulares o la PSTN.
Para este objetivo, lo más importante son las conexiones, los usuarios remotos van a poder tener acceso a los recursos de la red del sitio central, para poder entrar a las aplicaciones de datos que se manejan en la empresa, como son: levantamiento de pedidos, facturación, existencia de mercancía, etc.

Se muestra un diagrama con el cual está la solución propuesta:
(Ver anexo B)

Como se ve en el diagrama de la figura del anexo, se integrará en la solución un router de servicios integrados, además de proporcionar el servicio de Internet, nos proporcionara el servicio de un conmutador (PBX), vamos a tener dos tarjetas de interconexión FXO y FXS.
Las tarjetas FXO van a recibir las troncales analógicas del proveedor de servicios, las cuales van ayudarnos a tener salida hacia la PSTN. Las tarjetas FXS tendrán conectadas equipos analógicos como teléfonos y equipo de fax.

Para parte de los servicios de datos, el router será conectado por cable UTP hacia un equipo switch el cual proporcionara servicio de datos a todos los dispositivos de la red como son puntos de acceso, servidores, teléfonos IP, PC´s, e impresoras.

Y por último, para la parte de los usuarios remotos, el router tiene la capacidad de recibir túneles de VPN, el cual nos ayudará a extender nuestra red hacia ellos para tener acceso a las aplicaciones de nuestros servidores, manteniéndola segura y eficaz, ya que la información que se trasmita viajara por medios no seguros como es el Internet. Para la parte de telefonía IP, los usuarios se conectaran por medio de un software instalado en las computadoras portátiles llamado softphone, mediante el cual se registrará al router para establecer la conexión de VPN, automáticamente nos dará una extensión y el servicio de telefonía hacia la PSTN, todo esto siempre y cuando estemos registrados en el router. Con todo lo anterior se reducirán considerablemente los costos de telefonía; este proceso funciona inversamente, por ejemplo cualquier cliente que llame hacia nuestra red, podrá comunicarse con cualquier persona sin importar el lugar y momento donde se encuentre, sin necesidad de gastar en celular ó larga distancia.

5.4.- PLANEACIÓN

Para la realización de implementación de telefonía IP sobre una VPN, se necesitaran cubrir las necesidades de comunicación a bajo costo, de todos los usuarios incluyendo el personal que se conectara remotamente, y se propone la siguiente planeación:

a) Instalación y configuración inicial del Router
b) Configuración del servidor de DHCP en el router
c) Configuración de la conexión a Internet en el router
d) Configuración del servidor de VPN en el router
e) Configuración del Call Manager Express en el router
f) Instalación y configuración del cliente de VPN (Cisco Client) a los usuarios remotos
g) Instalación y configuración del softphone (IP Communicator) a los usuarios

5.5.- DESARROLLO.

5.5.1.- INSTALACIÓN Y CONFIGURACIÓN INICIAL DEL ROUTER.

PASOS A SEGUIR:

1.-Establecer comunicación con el router para configurarlo.
Conectar el cable de consola del router en la interfaz consola que se encuentra en la parte posterior del equipo. El cable de consola tiene en un extremo un conector serial y en el otro extremo un conector RJ-45 que debe de ir hacia el router.

2.-Conectamos el otro extremo del cable al puerto serial del computador con el cable extensor serial.

3.-Abrir el Hyperterminal de Windows:

Inicio>Programas>Accesorios>Comunicaciones>Hyperterminal.

4.-En la ventana *Nueva Conexión,* seleccionamos cualquier nombre para la conexión y hacemos clic en Aceptar. (ver anexo C)

5.-En la ventana de *Conectar a* hacemos clic en aceptar. Esto tomará el puerto serial al cual está conectado el cable de consola para hacer la conexión (ver anexo D).

6.-Luego en la ventana *Propiedades del COM1* hacemos clic en *Restaurar predeterminados* para entablar una comunicación a 9600 bits por segundo, 8 bits de datos, 1 bit de parada, etc., como se muestra en la figura (ver anexo E).

7.-Luego presionamos la tecla *Enter* para que se establezca la conexión con el *Router*.
Deberá aparecer en Hyper terminal la palabra Router como se muestra en la Figura (ver anexo F).

Después de haber realizado los pasos anteriores el *Router* ya está listo para recibir los comandos de configuración.

5.5.2.- SERVIDOR DHCP EN EL ROUTER.

Es necesario configurar un servidor DHCP en el router ya que este nos servirá para la asignación dinámica de las direcciones IP que serán utilizadas tanto por los usuarios locales, así como para los usuarios remotos (VPN) para que se puedan registrar en el call manager y tengan acceso a los recursos de la red LAN.

Para crear nuestro servidor DHCP es necesario tomar en cuenta algunos aspectos importantes:

- Las direcciones IP que no serán asignadas vía DHCP evitaran con esto, problemas de duplicidad de direcciones, ya que en algunos de nuestros equipos activos y servidores tendremos asignadas algunas direcciones IP en forma estática.
- El nombre que le asignaremos al pool de direcciones, para su fácil identificación ya que lo usaremos en configuraciones posteriores.
- La dirección IP de nuestra subred y su máscara de red corresponderán a nuestro pool de direcciones.
- La dirección ip de nuestro default router, es el que nos proporcionara el ruteo a redes desconocidas.
- La dirección ip de nuestro servidor DNS, es el que nos proporciona el servicio de conversión, nombres de dominio a direcciones IP.

En primer lugar configuraremos las direcciones IP que excluiremos de nuestro pool de direcciones, para ello es necesario acceder al modo de configuración global del router y escribir el comando "*ip dhcp excluded-address* ***ip-address***"
Posteriormente configuramos el nombre de nuestro pool de direcciones ip con el comando en modo de configuración global "*ip dhcp pool* ***pool-name",*** enseguida configuramos la subred con su respectiva mascara de red a la que pertenecerá

nuestro pool de direcciones, esto lo haremos estando dentro de la configuración de nuestro pool de direcciones ip con el comando “network ***network-address network-mask”,*** el siguiente paso es configurar el que será nuestro default router, recordando que esta dirección ip debe de estar dentro de las direcciones ips excluidas del pool de direcciones, ya que esta será asignada de forma estática al router y así evitamos duplicidad de direcciones, el comando que usaremos será el siguiente “default-router ***ip*** address” y por último configuraremos la dirección ip del que será nuestro servidor DNS, por medio del comando “dns-server ip-address”.

De esta forma queda configurado nuestro servidor DHCP, a continuación configuraremos la conexión a internet de nuestro ruteador, para ello usaremos una tarjeta Wic-dsl y un enlace ADSL de nuestro proveedor de servicios.

5.5.3.- LA CONEXIÓN A INTERNET EN EL ROUTER.

En este punto, se tiene contratado un servicio de Internet que provee una dirección dinámica, la cual cambia aleatoriamente, por esta razón necesitamos que esas direcciones se re-direccionen hacia un servidor de DNS, el cual empalme la dirección publica que está cambiando constantemente con el dominio en el servidor DNS. Para resolver esto, se hace uso de un servicio gratuito que nos ayuda con esto, la página de donde se configuro este servicio es www.dyndns.com.

Una vez teniendo la dirección IP pública re-direccionada con un dominio, el cual podremos accesar desde cualquier parte de Internet, necesitamos que nuestro equipo tome esa dirección para poder establecer la conexión de VPN. La configuración la hacemos desde el ROUTER CISCO 2801, el cual tiene instalada una tarjeta ADSL donde se recibe el servicio de internet del proveedor. Según el proveedor de servicio que se tenga, es el tipo de configuración que se realiza, sobre todo en la parte de PVC, y la autentificación. Se muestra un diagrama donde está la solución propuesta: (Ver anexo K).

5.5.4.- SERVIDOR VPN EN EL ROUTER.

Para ofrecer el servicio de conexión VPN a varios usuarios, necesitamos configurar el ROUTER CISCO 2801 como un servidor de VPN´s, el cual reciba, acepte y realice la conexión a los usuarios registrados para tener esta aplicación. Primero se deberá configurar la parte de autentificación y se crean los usuarios que vayan a realiza la conexión. Después se realiza la configuración del nombre de la conexión y la contraseña para la autentificación, y se asocian varios parámetros que tomaran lo equipos cuando se conectan, como la dirección IP, mascara de red, entre otras. No se debe olvidar el tipo de encripción que se va a manejar. A continuación se muestra la configuración del router para recibir 4 conexiones al mismo tiempo. Se muestra un diagrama donde está la solución propuesta: (Ver anexo K).

5.5.5.- CALL MANAGER EXPRESS EN EL ROUTER.

Una vez configurado el servidor DHCP, la conexión a Internet y el servidor de VPN es momento de configurar nuestro call manager Express, que será nuestro conmutador de Voz IP, para ello será necesario que accedamos al modo de configuración global de nuestro ruteador y usemos el comando "telepony-service", este comando nos va a permitir configurar todas las opciones de nuestra aplicación de telefonía virtual, para nuestro caso de estudio configuraremos primero la cantidad de teléfonos que usaremos, lo cual lo haremos con el comando "*max-ephones* ***ephone-number"*** posteriormente configuramos la cantidad de registros que usaremos en nuestro directorio, por medio del comando "*max-dn* ***dn-number",*** después de configurar la cantidad de registros es necesario configurar la dirección ip del call manager, para esto usamos el comando "ip source-address ***ip-address*** *port* ***port-number",*** esta dirección IP es importante ya que es la que usaran tanto nuestros teléfonos IP como en el softphone instalado a nuestras computadoras portátiles, para poder registrarse y les sea asignada una línea para poder realizar las llamadas. El siguiente paso en la configuración es asignar la cantidad máxima de conferencias que podremos realizar, para esto usamos el comando "max-conferences conferences-number", y por último configuramos un nombre de usuario y un password para poder administrar el call manager por medio de una interface Web, con el comando "web admin system name username password", con esto terminamos la configuración inicial de nuestro call manager, ahora daremos paso a la configuración de nuestro directorio. Se muestra un diagrama donde está la solución propuesta: (Ver anexo K).

En esta sección se describe la configuración del directorio que usaremos, el cual contempla los siguientes parámetros:

- Numero del registro (dn)
- Número de extensión.
- Nombre del registro.

Para configurar nuestro directorio accederemos al modo de configuración global de nuestro ruteador y usamos el comando "*ephone-dn* ***dn-number type-line",*** al ejecutar este comando accederemos al modo de configuración de número de directorio, estando dentro de este modo de configuración usamos el comando "number ***extensión-number",*** para asignar el número de extensión, y finalmente para asignarle un nombre usamos el comando "*name* ***username".*** Repetiremos los pasos anteriores para todos los registros que queramos configurar en nuestro directorio, una vez terminado el directorio es momento de configurar los teléfonos para que puedan registrarse en el call manager. Se muestra un diagrama donde está la solución propuesta: (Ver anexo K).

Una vez configurado el directorio es momento de configurar los parámetros de cada uno de los teléfonos tanto ip como softphone que usaremos, los parámetros que configuraremos en nuestro caso de estudio son los siguientes:

- Modo de seguridad.
- Dirección física del dispositivo que se registrará en el call manager.

- El codéc de compresión que usaremos para la voz.
- El tipo de teléfono.
- La línea o líneas que le serán asignadas a los teléfonos.

Para poder configurar los teléfonos en necesario acceder al modo de configuración global y usar el comando "*ephone* ***ephone-number",*** con este comando accederemos al modo de configuración del teléfono, es ahí en donde configuraremos los parámetros antes indicados para cada uno de los teléfonos. En primer lugar configuramos el modo de seguridad con el comando "*device-security-mode* ***mode",*** para configurar la dirección física del dispositivo usamos el comando "*mac-address* ***mac-address",*** para la configuración del códec usamos el comando "*codec* ***códec-type",*** este comando nos permite selecciona entre 3 tipos de condecs de compresión de voz, en nuestro caso seleccionamos el g729 ya que es el que mejor calidad nos dio con respecto al ancho de banda que estamos manejando, para asignar el tipo de teléfono usamos el comando "*type* ***ephone-type",*** con este comando podemos elegir entre una variedad de tipos de teléfonos ip, y por ultimo para asignarle las líneas que le corresponden al teléfono usamos el comando "*button* ***button-number : line-number",*** para configurar cada teléfono repetiremos los pasos anteriores, y así damos por terminada la configuración de nuestro call manager y estamos listos para iniciar las llamadas usando la tecnología de voz ip, ahora solo resta configurar las líneas analógicas y los teléfonos analógicos para hacer la integración de la telefonía tradicional y la voz ip. Se muestra un diagrama donde está la solución propuesta: (Ver anexo K).

5.5.6.- INSTALACIÓN Y CONFIGURACIÓN DEL CLIENTE DE VPN (CISCO CLIENT) A LOS USUARIOS REMOTOS.

Para instalar el cliente VPN, debe proceder de la siguiente forma:
1.- Ejecutar la aplicación de instalación vpnclient_setup.exe. En la siguiente ventana, presionar "Next" (ver anexo G)
2.- En la ventana de "License Agreement", seleccionar "I accept de license agreement" y presionar el botón "Next" (ver anexo G)
3.- En la siguiente ventana, deberá seleccionar el directorio donde desea que se instalen los componentes de la aplicación mediante el botón "Browse". Por omisión, el instalador seleccionará el directorio de Programas de Windows. Ya sea que se utilice el directorio propuesto o se seleccione otro, presionar el botón "**Next**"
4. Volver a presionar el botón "**Next**" en las siguientes ventanas para iniciar con el proceso de instalación y finalmente, reiniciar el equipo de cómputo.

Conexión a la Red Privada Virtual

Una vez finalizada la instalación y reiniciado el equipo de cómputo, se podrá establecer una conexión a la Red Privada Virtual mediante el siguiente procedimiento:
1.- Ejecutar la aplicación "**VPN Client**", la cual se localiza en el menú de inicio de Windows, dentro de la carpeta de "Todos los programas" la llamada "**Cisco Systems VPN Client**".
2. Se presentará una ventana como la fig (ver anexo H)
3. Dar clic en el la opción "**New**". Y llenar el cuadro de dialogo

Donde; "**Description"** es el nombre del Usuario que se le esta previamente asignado y configurando en el router para la VPN, "**Password y Confirm Password**".
Ahora de click en la pestaña "**Transport**" . Aquí solo seleccionar la opción "**IPSec over"** TCP con el "**TCP Port: 10000"**.
Y por ultimo dar click en "**Save**"
4.- Bajo la sección "**Connection Entries**", notará que ya existe un "**Conection Entry**" de nombre "Usuario"
6.- Deberá presionar el botón "**Connect**" señalado en la figura anterior. En unos segundos deberá presentarse una ventana. (ver anexo H)
7.- Esta ventana solicitará un "**Username**" y **Password**" que corresponde a la cuenta de usuario de VPN y clave de acceso que el Administrador ha proporcionado a los Usuarios, presionar el botón "**OK**"
8. En este punto, el cliente VPN intentará establecer una conexión con la Red Privada Virtual. De completarse la conexión satisfactoriamente, se presentará un mensaje indicando "**CONEXIÓN ACEPTADA**".

5.5.7.- INSTALACIÓN Y CONFIGURACIÓN DEL SOFTPHONE (IP COMMUNICATOR) A LOS USUARIOS.

Para instalar el IP Communicator, debe proceder de la siguiente forma:
1.- Ejecutar la aplicación de instalación CiscoIPSoftphoneSetup.exe.
En la siguiente ventana, presionar "Next" (ver anexo I)
2.- En la ventana de "License Agreement", seleccionar "I accept de license agreement" y presionar el botón "Next" (ver anexo I).
3.- En la siguiente ventana, deberá seleccionar el directorio donde desea que se instalen los componentes de la aplicación mediante el botón "Browse". Por omisión, el instalador seleccionará el directorio de Programas de Windows. Ya sea que se utilice el directorio propuesto o se seleccione otro, presionar el botón "**Next**"

4. En la ventana "Ready to install the program" presionar el botón "Install" para iniciar el proceso de instalación (ver anexo I)
5. Volver a presionar el botón "Next" en las siguientes ventanas para continuar con el proceso de instalación
6. Termino de instalación (ver anexo I)

Configuración del IP COMUNICATOR.

Una vez finalizada la instalación y reiniciado el equipo de cómputo, se podrá iniciar la aplicación del IP Comunicator la primera vez que se inicia solicita la configuración siguiente:
1.- Ejecutar la aplicación", la cual se localiza en el menú de inicio de Windows, dentro de la carpeta de "Todos los programas" la llamada "IP Comunicator". (ver anexo J)
2. En la ventana de "select and tune device presionar el botón "Next" (ver anexo J)
3. En la siguiente ventana personalizaremos nuestro equipo, presionar el botón "Next" (ver anexo J)
4.-En la ventana "Adjust the listening Volume", ajustaremos el audio, presionar el botón "Next" (ver anexo J)

5.-En la ventana “Adjust the microphone Volume”, ajustamos el volumen deseado para el micrófono, presionar el botón “Next” (ver anexo J)
6.-Al termino de la configuración aparecerá la ventana siguiente (ver anexo J)
7.-La siguiente ventana es el softphone de cisco con el cual al iniciarlo y estar previamente configurado en el router el numero asignado de acuerdo a la dirección MAC del equipo , intentará establecer una conexión con el router ya sea por LAN o por VPN

CONCLUSIÓN.

La necesidad de que las empresas cuenten con la información relevante de sus negocios se ha vuelto una constante en la realización de soluciones que hagan que los usuarios de las empresas tengas las herramientas para poder tomar decisiones en cualquier lugar y situación, acercando virtualmente sus oficinas para tener acceso a sus aplicaciones, contactos, correo, entre otras cosas, en cualquier lugar donde se encuentren por medio del Internet.

Esta tesina está desarrollada sobre ese principio que consiste en tener disponible la información vital de las empresas a cualquier hora y en cualquier lugar, la evolución ha cambiado la forma de hacer negocios, así como las necesidades de las empresas van más allá, no solamente necesitan el acceso a sus aplicaciones, además la comunicación entre las oficinas con los usuarios remotos es primordial.

Este proyecto se diseño para que se tengan cubiertas las necesidades de voz y datos a un bajo costo, en un mediano y largo plazo.

Lo analizado en este tema es solo parte de la integración con la que actualmente se encuentran los usuarios y empresas conectados a los sistemas de comunicación móviles privados, los cuales podemos destacar como: la movilidad en accesos de banda ancha, mensajería instantánea 3G; tenemos presente que la idea no es dejar de utilizar los servicios tradicionales de telefonía y mensajería, sino todo lo contrario aportar, mejorar e implementar comunicaciones con calidad y confiabilidad.

ANEXO A

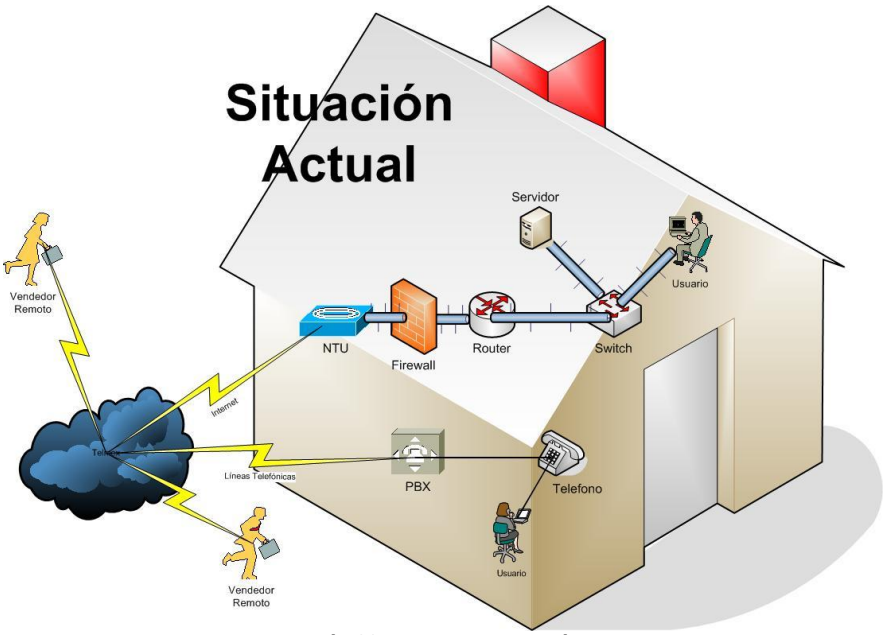


Fig 28. Esquema Actual

ANEXO B

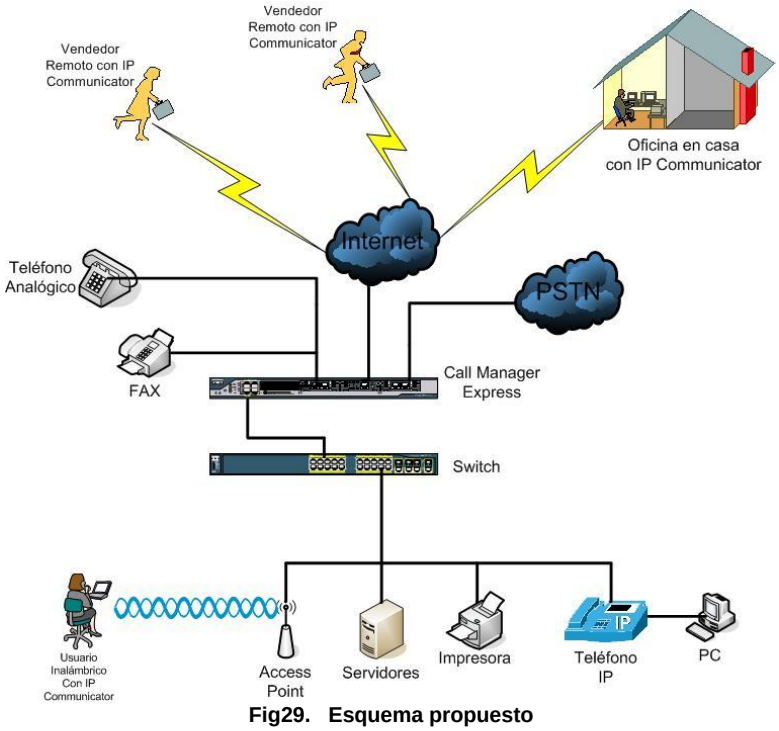


Fig29. Esquema propuesto

ANEXO C.

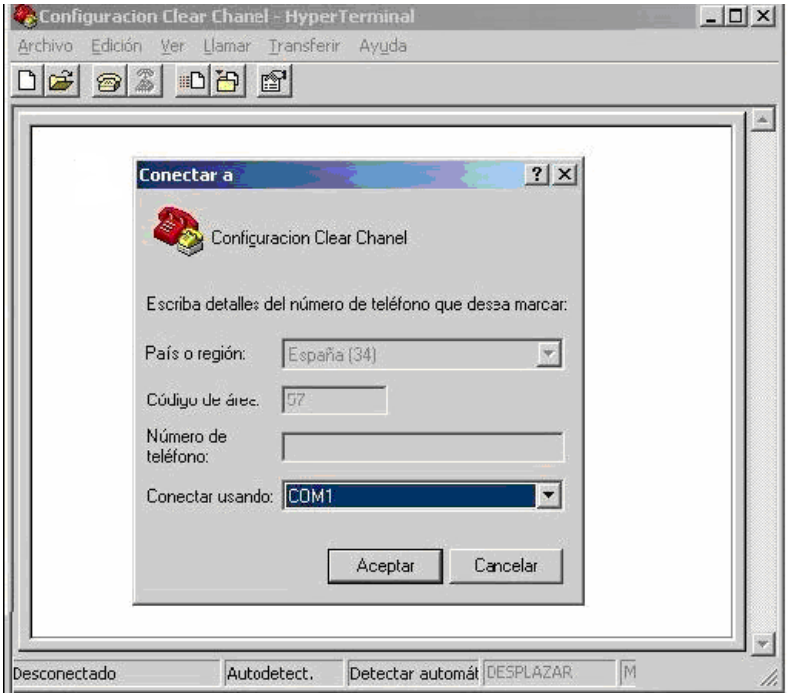


Fig.30.-Configuración Hyper Terminal.

ANEXO D.

Fig 31..-Descripción de la conexión.

ANEXO E.

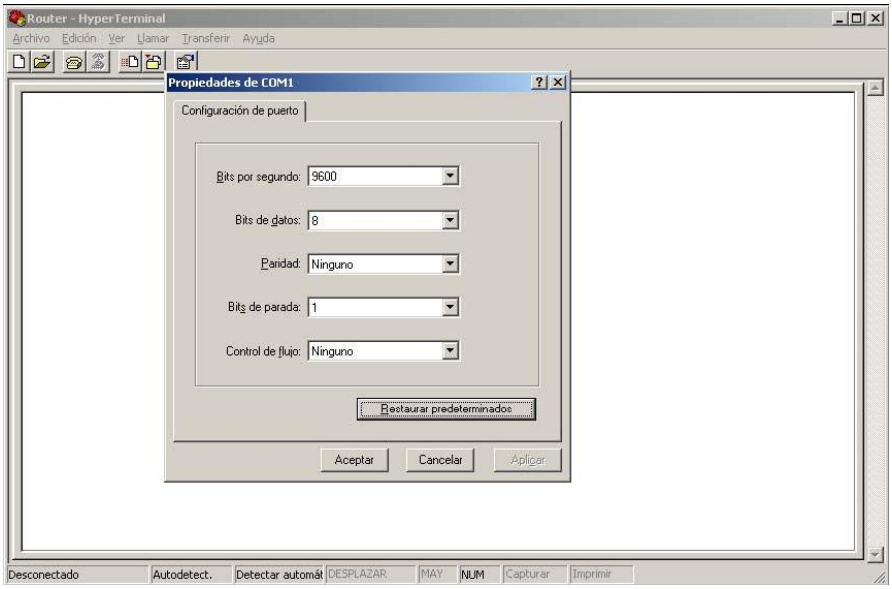


Fig32..-Propiedades del COM1.

ANEXO F.

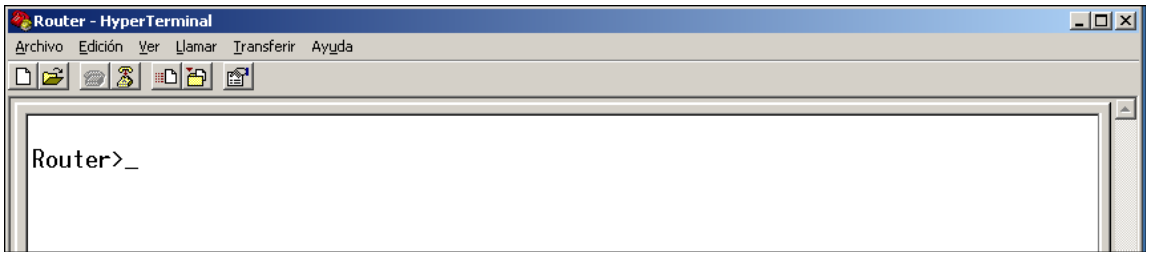


Fig33..-Conexión con el router.

ANEXO G

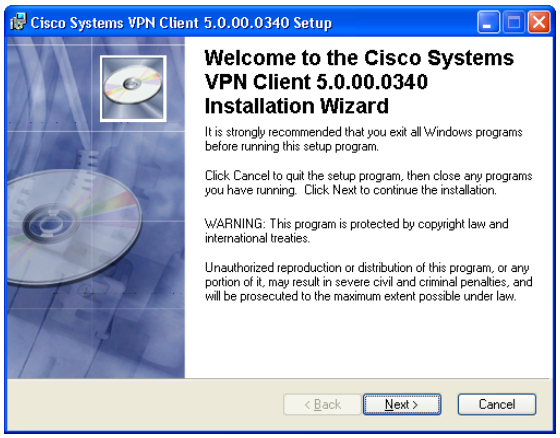


Fig 34 Ejecutar aplicación

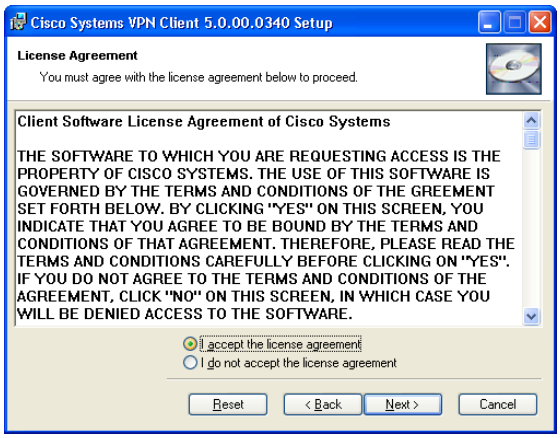


Fig 35 Acuerdo de Licencia

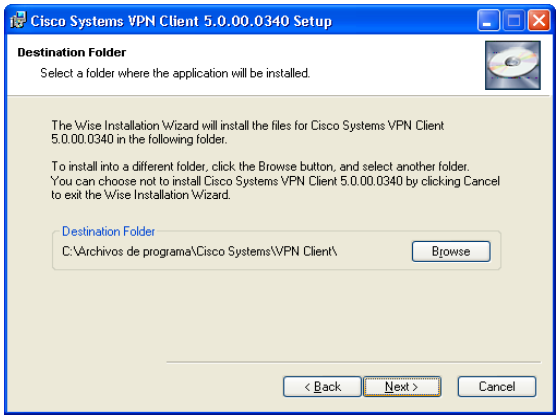


Fig 36 Seleccionando el directorio para instalación

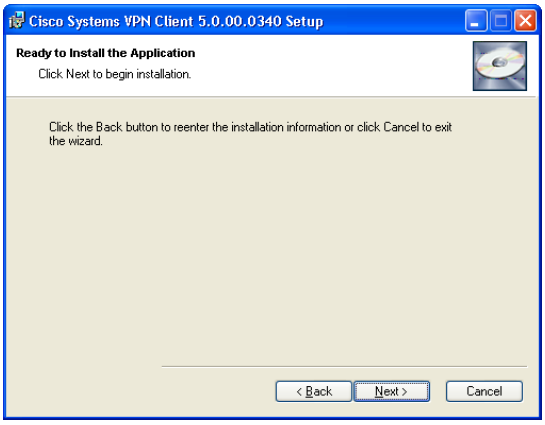
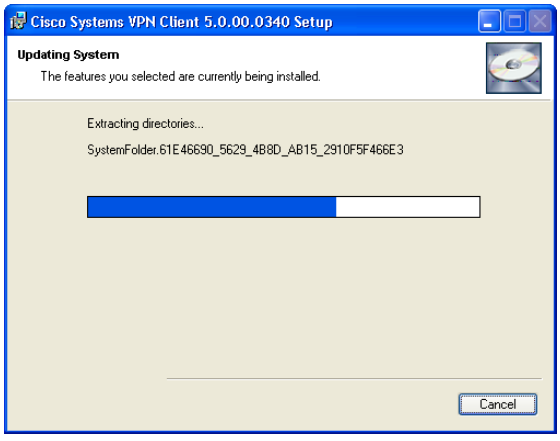


Fig37 Ejecutar aplicación



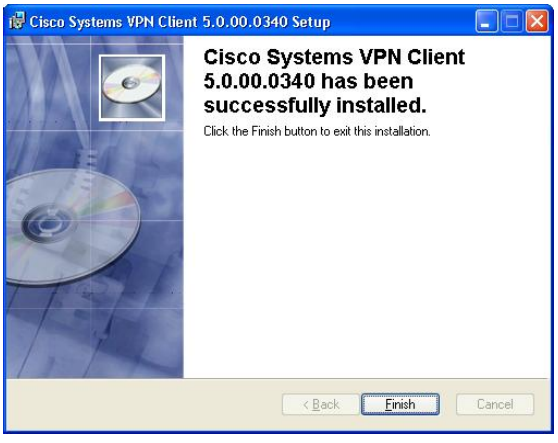


Fig 38 Proceso de Instalación

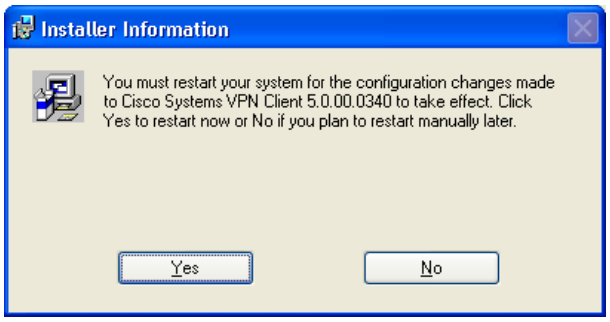


Fig39..-Reinicio de Sistema.

ANEXO H

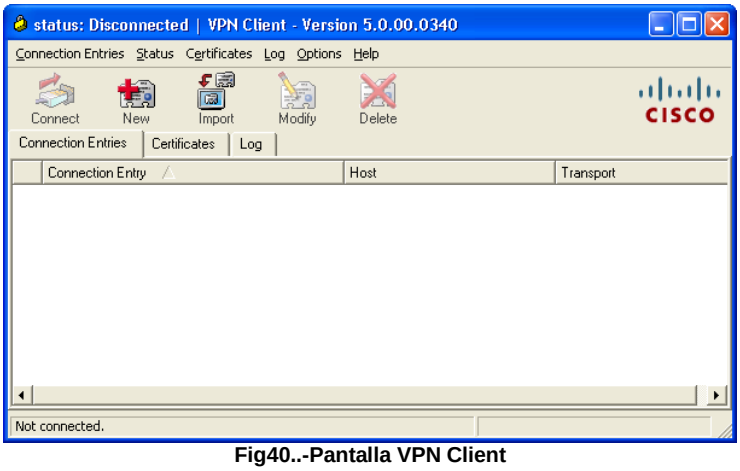


Fig40..-Pantalla VPN Client

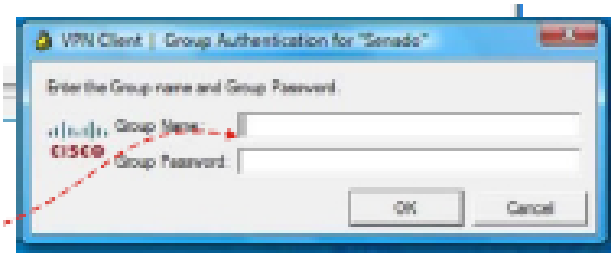


Fig41..-Introducir Username y Password asignados

ANEXO I

Fig 42 Ejecutar aplicación

Fig 43 Acuerdo de Licencia

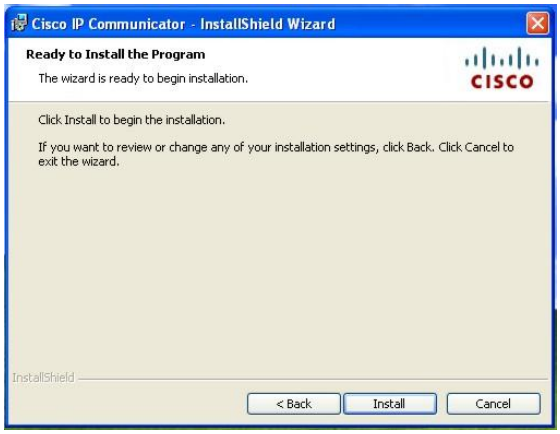


Fig 44 Confirmación de instalación

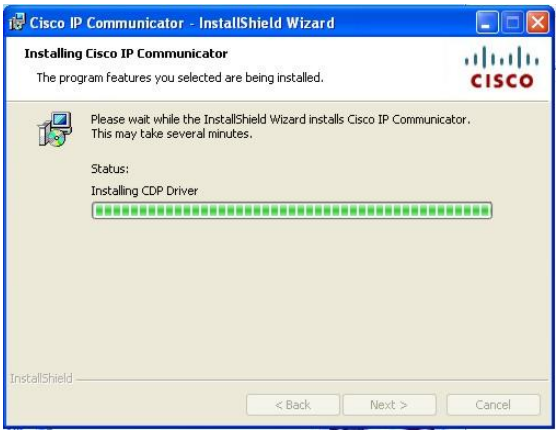


Fig 45 Proceso de Instalación

Fig46 Término de Instalación

ANEXO J

Fig 47 Inicio de configuración

Fig48 configuración

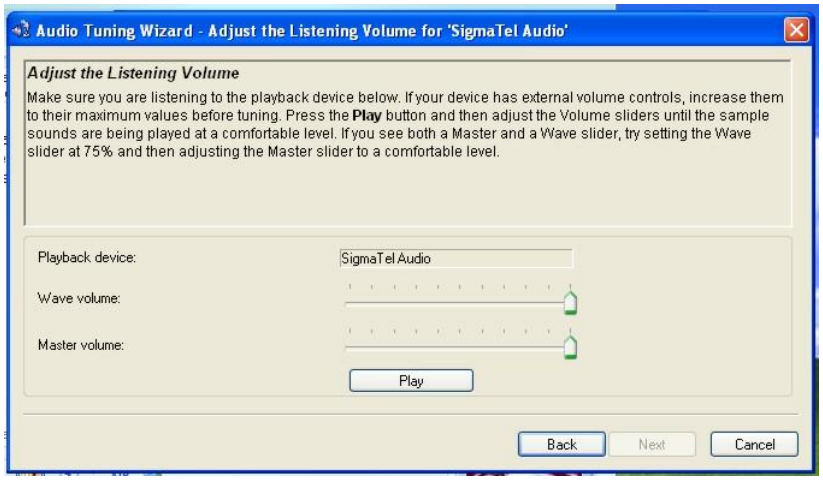


Fig49 Configuración de Audio

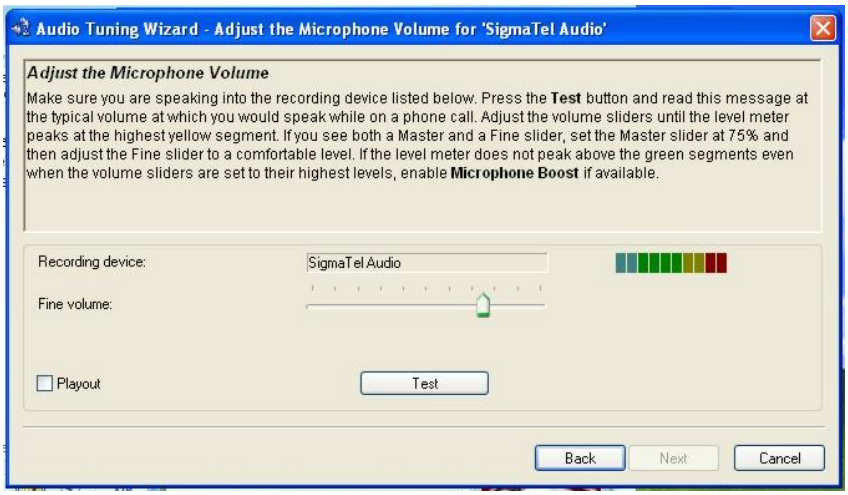


Fig50 Configuración de VOZ

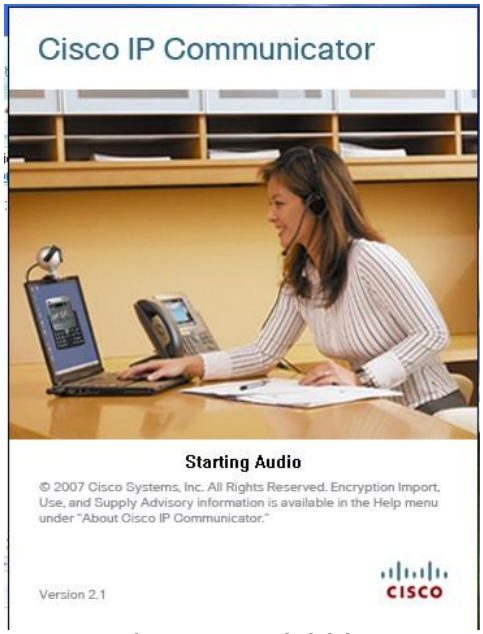


Fig51 Ventana de inicio

Fig 52 Softphone

ANEXO K

```
 ++++++++++++++++++++++++++++++++++++++++++++++
+                                              +
+                  ---------------------------- +
+                  C I S C O  S Y S T E M S     +
+                  ---------------------------- +
+                                               +
+                                 | |           +
+                                ||| |||        +
+                               ||||| |||||      +
+                           .:|||||||:...:|||||||:.           +
+          WELCOME TO THE HUMANE NETWORK   +
+                                               +
+                  SEMINARIO DE TITULACION      +
+                          I P N                +
+                                               +
++++++++++++++++++++++++++++++++++++++++++++++++      //Mensaje de Advertencia

ADVERTENCIA!!!!!!!!
EL ACCESO A ESTE EQUIPO ESTA RESTRINGIDO, Y
TIENE MONITOREO CONSTANTE, SOLAMENTE PERSONAL
AUTORIZADO TIENE DERECHO A INGRESAR.


no ip dhcp use vrf connected
ip dhcp excluded-address 10.10.1.250 10.10.1.254  //Direcciones IP Reservadas
ip dhcp excluded-address 10.10.1.1
!
ip dhcp pool MI_RES                               //Configuración del Servidor DHCP
  network 10.10.1.0 255.255.255.0
  default-router 10.10.1.254
  dns-server 200.33.146.193 200.33.146.201
!
ip name-server 200.33.146.193
ip name-server 200.33.146.201
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
voice-card 0
!
username chavin privilege 15 password 7 121A0C041104  //Usuarios Locales
username choco privilege 15 password 7 05080F1C2243
username edyboy privilege 15 password 7 104D000A0618
username jordan privilege 15 password 7 121A0C041104
archive
 log config
```

```
  hidekeys
!
crypto isakmp policy 3                                  //Empieza la configuración de la VPN
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp client configuration group clientevpn          //Parámetros de la VPN
 key seminario
 pool IPs_VPN
 acl 102
 max-users 4
 netmask 255.255.255.0
!
crypto ipsec transform-set MIVPN esp-3des esp-md5-hmac
!
crypto dynamic-map MI_MAP_VPN 10
 set transform-set MIVPN
 reverse-route
!
crypto map clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list groupauthor
crypto map clientmap client configuration address respond
crypto map clientmap 10 ipsec-isakmp dynamic MI_MAP_VPN
!
interface FastEthernet0/0
 ip address 10.10.1.254 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 ip tcp adjust-mss 1412
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface ATM0/2/0                              //Configuración de Internet
 no ip address
 no atm ilmi-keepalive
 dsl operating-mode auto
!
interface ATM0/2/0.1 point-to-point
 pvc 8/81
  oam-pvc manage
  pppoe-client dial-pool-number 1
interface Dialer0                               //Configuración de Internet
```

```
 ip address negotiated
 ip mtu 1452
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 no cdp enable
 ppp authentication chap pap callin
 ppp chap hostname famlealbetanzos21
 ppp chap password 7 0828484B044B5447455B5B
 ppp pap sent-username xxxxxxxxxxxxx password 7 xxxxxxxxxxxxxxx
 crypto map clientmap
!
ip local pool IPs_VPN 10.10.1.250 10.10.1.253
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 Dialer0
!
!
ip http server
no ip http secure-server
ip http path flash                                    //Configuración de NAT
ip nat inside source route-map Cliente_VPN interface Dialer0 overload

!
access-list 1 permit 10.10.1.0 0.0.0.255              //Configuración de las reglas del control
de trafico de la red
access-list 101 deny   ip any 10.10.1.248 0.0.0.7
access-list 101 deny   ip 10.10.1.0 0.0.0.255 10.10.1.248 0.0.0.7
access-list 101 permit ip 10.10.1.0 0.0.0.255 any
access-list 102 permit ip 10.10.1.0 0.0.0.255 any
access-list 103 permit tcp any any eq 2000
access-list 104 permit udp any any range 16384 32768

route-map Cliente_VPN permit 1
 match ip address 101
!
control-plane
!
voice-port 0/0/0                                      //Configuración de una extensión analógica
 signal loopStart
 ring cadence pattern02
 input gain 3
 output attenuation -2
 echo-cancel coverage 32
 cptone MX
!
voice-port 0/0/1
 signal loopStart
```

```
dial-peer voice 1111 pots                    //Configuración de una extensión analógica
 destination-pattern 1111
 port 0/0/0
!
gateway
 timer receive-rtp 1200
!
Router(config)#telephony-service             //Configuración del Call Manager

*/ Se configure la cantidad de teléfonos y números que se van a usar */

Router(config-telephony)#max-ephones 6
Router(config-telephony)#max-dn 6

*/ Dirección ip del call manager al que se van a registrar los teléfonos */

Router(config-telephony)#ip source-address 10.10.1.254 port 2000

*/ Cantidad máxima de conferencias */

Router(config-telephony)#max-conferences 8 gain -6

*/ Usuario para administración via web */

Router(config-telephony)#web admin system name chavinter secret 5
$1$v6yj$o20aaXeZ.CnmjPQIeuIZt0

Router(config-telephony)#transfer-system full-consult
!
ephone-dn  1  dual-line                      //Configuración de las extensiones
 number 5001
 name Sergio
!
ephone-dn  2  dual-line
 number 5002
 name Oscar
!
ephone-dn  3  dual-line
 number 5003
 name Perla
!
ephone-dn  4  dual-line
 number 5004
 name Israel
!
ephone-dn  5  dual-line
 number 5005
 name EdyBoy
!
```

```
ephone-dn  6  dual-line
 number 5006
 name Jordan
!
ephone  1                          //Configuración de las extensiones
 device-security-mode none
 mac-address 0016.D49C.847E
 codec g729r8
 type 7960
 button  1:1
!
ephone  2
 device-security-mode none
 mac-address 0005.9A3C.7800
 codec g729r8
 type 7960
 button  1:2
!
ephone  3
 device-security-mode none
 mac-address 00C0.9FF5.5B4A
 codec g729r8
 type 7960
 button  1:3
!
ephone  4
 device-security-mode none
 mac-address 00E0.9113.F0A5
 codec g729r8
 type 7960
 button  1:4
!
ephone  5
 device-security-mode none
 mac-address 0014.228B.2619
 codec g729r8
 type 7960
 button  1:5
!
ephone  6
 device-security-mode none
 mac-address 000D.5678.337B
 codec g729r8
 type 7960
 button  1:6
!
line con 0
 password 7 0822455D0A16
line aux 0
```

```
line vty 0 4
 password 7 110A1016141D
!
scheduler allocate 20000 1000
end
```

ANEXO L

INDICE DE FIGURAS Y CUADROS.

GLOSARIO.

***ATM*.** Asynchronous Transfer Mode (Modo de Transferencia Asíncrona).

CCITT. Consultative Committee for International Telegraph and Telephone (Comité Consultivo Internacional de Telefonía y Telegrafía).

***CPE*.** Customer Premises Equipment (Equipo en Instalaciones de Cliente).

CTI. Computer Telephony Integration (Integración Ordenador- Telefonía).

DiffServ. Differentiated Services Internet QoS model (modelo de Calidad de Servicio en Internet basado en Servicios Diferenciados).

DNS. Domain Name System (Sistema de Nombres de Dominio).

E.164. Recomendación de la ITU-T para la numeración telefónica internacional, especialmente para ISDN, BISDN y SMDS..

ENUM .Telephone Number Mapping (Integración de Números de Teléfono en DNS).

FDM. Frequency Division Multiplexing (Multiplexado por División de Frecuencia).

FoIP. Fax over IP (Fax sobre IP).

H.323. Estándar de la ITU-T para voz y videoconferencia interactiva en tiempo real en redes de área local, LAN, e Internet.

IETF. Internet Engineering Task Force (Grupo de Trabajo de Ingeniería de Internet).

IGMP. Internet Group Management Protocol (Protocolo de Gestión de Grupos en Internet).

IN. Intelligent Network (Red Inteligente).

IntServ. Integrated Services Internet QoS model (modelo de Calidad de Servicio en Servicios Integrados de Internet).

IP. Internet Protocol (Protocolo Internet).

IP Multicast. Extensión del Protocolo Internet para dar soporte a comunicaciones multidifusión.

IPBX. Internet Protocol Private Branch Exchange (Centralita Privada basada en IP).

IPSec. IP Security (Protocolo de Seguridad IP).

ISDN. Integrated Services Data Network (Red Digital de Servicios Integrados, RDSI).

ISP. Internet Service Provider (Proveedor de Servicios Internet, PSI).

ITSP. Internet Telephony Service Provider (Proveedor de Servicios de Telefonía Internet, PSTI).

ITU-T. International Telecommunications Union - Telecommunications (Unión Internacional de Telecomunicaciones- Telecomunicaciones).

LDP. Label Distribution Protocol (Protocolo de Distribución de Etiquetas).

LSR. Label Switching Router (Encaminador de Conmutación de Etiquetas).

MBONE. Multicast Backbone (Red Troncal de Multidifusión).

MCU. Multipoint Control Unit (Unidad de Control Multipunto).

MEGACO. Media Gateway Control (Control de Pasarela de Medios).

MGCP. Media Gateway Control Protocol (Protocolo de Control de Pasarela de Medios).

MOS. Mean Opinion Score (Nota Media de Resultado de Opinión).

MPLS. Multiprotocol Label Switching (Conmutación de Etiquetas Multiprotocolo).

OLR. Overall Loudness Rating (Índice de Sonoridad Global).

PBX. Private Branch Exchange (Centralita Telefónica Privada).

PHB. Per Hop Behaviour (Comportamiento por Salto).

PoP. Point of Presence (Punto de Presencia).

POTS. Plain Old Telephone Service (Servicio Telefónico Tradicional).

PPP. Point to Point Protocol (Protocolo Punto a Punto).

PSTN. Public Switched Telephone Network (Red de Telefonía Conmutada Pública).

QoS. Quality of Service (Calidad de Servicio).

RAS. Registration, Authentication and Status (Registro, Autentificación y Estado).

RSVP. Reservation Protocol (Protocolo de Reserva).

RTCP. Real Time Control Protocol (Protocolo de Control de Tiempo Real).

RTP. Real Time Protocol (Protocolo de Tiempo Real).

SAP. Session Annunciation Protocol (Protocolo de Anuncio de Sesión).

SCN. Switched Circuit Network (Red de Circuitos Conmutados).

SDP. Session Description Protocol (Protocolo de Descripción de Sesión).

SIP. Session Initiation Protocol (Protocolo de Inicio de Sesión).

SLA. Service Level Agreement (Acuerdo de Nivel de Servicio).

SS7. Signalling System Number 7 (Sistemas de Señales número 7).

STMR. Side Tone Masking Rating (Índice de Enmascaramiento para el Efecto Local).

TCP. Transmission Control Protocol (Protocolo de Control de Transmisión).

TDM. Time Division Multiplexing (Multiplexado por División de Tiempo).

TIPHON. Telecommunications and Internet Protocol Harmonization Over Networks (Armonización de Protocolos de Redes de Telecomunicación e Internet).

UDP. User Datagram Protocol (Protocolo de Datagramas de Usuario).

UMTS. Universal Mobile Telephone System (Sistema Universal de Telecomunicaciones Móviles).

VLAN. Virtual Local Área Network (Red de Área Local Virtual).

VPN. Virtual Private Network (Red Privada Virtual).

xDSL. Cualquiera de las tecnologías de Líneas de Suscripción Digital (por ejemplo, ADSL).

TÉRMINOS.

Circuit switching. (Conmutación de circuitos). Técnica de comunicación en la que se establece un canal (o circuito dedicado) durante toda la duración de la comunicación. La red de conmutación de circuitos más ubicua es la red telefónica, que asigna recursos de comunicaciones (sean segmentos de cable, «ranuras» de tiempo o frecuencias) dedicados para cada llamada telefónica.

Codec. (Códec). Algoritmo software usado para comprimir/ descomprimir señales de voz o audio. Se caracterizan por varios parámetros como la cantidad de bits, el tamaño de la trama (frame), los retardos de proceso, etc. Algunos ejemplos de codecs típicos son G.711, G.723.1, G.729 o G.726.

Extranet. (Extranet). Red que permite a una empresa compartir información contenida en su Intranet con otras empresas y con sus clientes. Las extranets transmiten información a través de Internet y por ello incorporan mecanismos de seguridad para proteger los datos.

Gatekeeper. (Portero). Entidad de red H.323 que proporciona traducción de direcciones y controla el acceso a la red de los terminales, pasarelas y MCUs H.323. Puede proporcionar otros servicios como la localización de pasarelas.

Gateway. (Pasarela). Dispositivo empleado para conectar redes que usan diferentes protocolos de comunicación de forma que la información puede pasar de una a otra. En VoIP existen dos tipos principales de pasarelas: la Pasarela de Medios (Media Gateways), para la conversión de datos (voz), y la Pasarela de Señalización (Signalling Gateway), para convertir información de señalización.

Impairments. (Defectos). Efectos que degradan la calidad de la voz cuando se transmite a través de una red. Los defectos típicos los causan el ruido, el retardo el eco o la pérdida de paquetes.

Intranet. (Intranet). Red propia de una organización, diseñada y desarrollada siguiendo los protocolos propios de Internet, en particular el protocolo TCP/IP. Puede tratarse de una red aislada, es decir no conectada a Internet.

IP Telephony. (Telefonía Internet). Ver «Voice over IP»

Jitter. (variación de retardo). Es un término que se refiere al nivel de variación de retado que introduce una red. Una red con variación 0 tarda exactamente lo mismo en transferir cada paquete de información, mientras que una red con variación de retardo alta tarda mucho más tiempo en entregar algunos paquetes que en entregar otros. La variación de retardo es importante cuando se envía audio o video, que deben llegar a intervalos regulares si se quieren evitar desajustes o sonidos ininteligibles.

Packet switching. (Conmutación de paquetes). Técnica de conmutación en la cual los mensajes se dividen en paquetes antes de su envío. A continuación, cada paquete se transmite de forma individual y puede incluso seguir rutas diferentes

hasta su destino. Una vez que los paquetes llegan a éste se agrupan para reconstruir el mensaje original.

Router. (Encaminador, enrutador). Dispositivo que distribuye tráfico entre redes. La decisión sobre a donde enviar los datos se realiza en base a información de nivel de red y tablas de direccionamiento. Es el nodo básico de una red IP.

Softswitch. (Conmutación por software). Programa que realiza las funciones de un conmutador telefónico y sustituye a éste al emular muchas de sus funciones de dirigir el tráfico de voz, pero además añade la flexibilidad y las prestaciones propias del tráfico de paquetes.

VoIP, Voice over IP. (Voz sobre IP). Método de envío de voz por redes de conmutación de paquetes utilizando TCP/IP, tales como Internet.

BIBLIOGRAFÍA.

1. BLACK, U. (1999). Voice over IP. New Jersey: Prentice Hall PTR.

2. CUERVO, F., GREENE, N., HUITEMA, C., RAYHAN, A., ROSEN, B. y SEGERS, J. (2000). Megaco Protocol versión 0.8. RFC 2885, Agosto 2000.

3. DOUSKALIS, B. (2000). IP telephony: the integration of robust VoIP services. New Jersey: Prentice Hall PTR.

4. GREENE, N., RAMALHO, M. y ROSEN, B. (2000). Media Gateways Control Protocol Architecture and Requeriments. RFC 2805, Abril 2000.

5. HAMDI, M., VERSCHEURE, O., HUBAUX, J-P., DALGIC, I. y WANG, P. (Mayo, 1999).Voice Service Interworking for PSTN and IP Networks. IEEE Communication Magazine, Mayo 1999, pags. 104-111.

6. HERSENT,O. GURLE, D. y PETIT, J.P. (2000). IP telephony: packet – based multimedia communication systems. Great Britain: Addison – Wesley.

7. ITU-T Study Group 16 (1998). Recommendation H.246. Enero 1998.

8. ITU-T Study Group 16 (2000). Recommendation H.323v4 (draft). Noviembre 2000.

9. MINOLI, D. y MINOLI, E. (1998). Delivering Voice over IP Networks. New York: John Wiley & Sons, Inc.

10. DAVISON JONATHAN, PETERS JAMES. Fundamentos de voz sobre IP (2001).

11. http://www.red.com.mx/scripts/resArticulo.php3?idNumero=64&articuloID=7460.

12. http://www.data.com/issue/981121/quality.html.

13. http://www.cisco.com/warmp/public/cc/cisco/mkt/wan/ipatm/tech/mpls_wp.htm.

14. http://www.cisco.com/warmp/public/cc/cisco/mkt/servprod/dial/tech/ievpn_rg.htm.

15. http://www.tendenciasdigitales.com