PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIÓN

PERFIL DEL TRABAJO PREVIO LA OBTENCION DEL TÍTULO DE:

MASTER EN REDES DE COMUNICACIÓN

TEMA:

DISEÑO DE UNA RED VPN PARA LA INTEGRACIÓN DE LOS SERVICIOS DE VOIP Y VIDEO VIGILANCIA PARA LOS INFOCENTROS COMUNITARIOS.

LIZET MARÍA RAMOS DILLON

Quito – 2016

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

1. INTRODUCCIÓN

La constitución de la república garantiza en varios de sus artículos, el derecho de todo ciudadano al acceso universal a las tecnologías de la información y comunicación, en virtud de esto el Ministerio de Telecomunicaciones y de la Sociedad de la Información como institución rectora en el área de las telecomunicaciones viene desde el año 2013 desarrollando proyectos de desarrollo social, con la dotación de centros de acceso a las tecnologías de la información y el conocimiento denominados Infocentros, estos centros se ubican a nivel nacional en las zonas rurales y urbano marginales de nuestro país, garantizando que el servicio llegue a las personas consideradas económicamente más vulnerables.

Sin embargo la tecnología instalada en cada Infocentro puede ser aprovechada para la instalación de otros sistemas que contribuyan al control, operación del Infocentro y la seguridad de sus actores, es por eso que se plantea este estudio para el diseño de una red VPN para la integración de los servicios de telefonía IP y video vigilancia.

El desarrollo del estudio se divide en cinco objetivos: empieza por el análisis de la situación actual del proyecto y de los parámetros de la red interna de cada Infocentro, se revisa los tipos de tecnologías utilizadas para la dotación de conectividad de los Infocentros y Megainfocentros, determinando que el diseño de la red VPN se la realizará sobre los Infocentros y Megainfocentros que disponen del enlace de internet por fibra óptica por su ancho de banda y aprovechamiento del equipamiento existente.

El desarrollo del segundo objetivo es la elección de equipos tanto para el sistema de VoIP como para el sistema de Video vigilancia, para esto se hace un breve repaso a las características que deben cumplir los equipos a ser seleccionados.

El tercer objetivo es el diseño de la red VPN, para la transmisión de voz, video y datos usando el internet como canales de transmisión, para esto se realiza una identificación de las tipologías de red VPN, hasta identificar la más apropiada para este diseño tomando en cuenta las necesidades del proyecto, mismas que serán analizadas en el primer objetivo.

En el cuarto objetivo se encuentra el cálculo del ancho de banda para el funcionamiento óptimo de cada sistema propuesto, para esto se analiza el tráfico que se generaría por el uso de estos dos

sistemas en un Infocentro o Megainfocentro así como el generado en la oficina central, que se encontrará ubicada en el MINTEL.

Como último objetivo se desarrolla el análisis de políticas de calidad de servicio QoS, que se aplicaría para los servicios de telefonía y video vigilancia, y se analizan los tipos de tráfico, modelos de calidad de servicio y métodos de implementación.

2. JUSTIFICACIÓN

La Constitución de la República del Ecuador, en su capítulo Segundo Derechos del Buen Vivir, sección tercera Comunicación e Información, establece que:

"Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. *Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos.*
2. *El acceso universal a las tecnologías de información y comunicación. " [1]*

El Ministerio de Telecomunicaciones y de la Sociedad de la Información como ente rector en esta área ha impulsado desde su creación proyectos que se enfoquen en reducir el analfabetismo digital en el país, es así que desde el año 2013 inicia el Proyecto Ampliación de la Red Infocentros, con la finalidad de dotar de un espacio de acceso a las tecnologías de la información y comunicación a los habitantes de zonas rurales y urbano marginales de nuestro país, a la presente fecha este Proyecto integra un total de 808 Infocentros y 25 Megainfocentros. [2]

Con este proyecto se ha buscado incrementar el desarrollo social y económico de la población de zonas rurales y urbano marginales, quienes son los que menor acceso tienen a las TIC's, un Infocentro.

Un Infocentro se define como "un espacios comunitarios de participación y desarrollo, que garantizan el acceso inclusivo a las Tecnologías de la Información y Comunicación de las poblaciones de parroquias rurales y urbanas marginales del Ecuador, la propuesta es introducir al ciudadano en el conocimiento de las TIC con el fin de reducir la brecha y analfabetismo digital, motivándole a emplear la tecnología para su aprovechamiento, mejorando así su calidad de vida

e impulsando el desarrollo productivo de su comunidad, propiciando el acceso a productos y servicios en línea, tanto locales como internacionales." [W12]

En un contexto general cada Infocentro se encuentra provisto de 10 computadores y un Megainfocentro posee 50 computadores que se encuentran al servicio de la ciudadanía, de la misma forma cada Infocentro dispondrá de una persona que se encargará de su atención y para el caso de los Megainfocentros se dispondrá de dos personas para este mismo fin.

El registro de asistencia de los facilitadores ha significado un problema para la dirección de este proyecto, la distancia entre cada Infocentro dificulta que el Gestor Social que es la persona encargada del control y operatividad de los Infocentros por cada provincia pueda evidenciar diariamente que todos los Infocentros estén en funcionamiento de acuerdo a sus horarios de Atención, actualmente cada Facilitador evidencia su asistencia a través de capturas de pantalla del control de velocidad del enlace de Internet, tarea que el facilitador debe realizarla diariamente una vez que empieza la atención a la ciudadanía.

Por otro lado, cada Infocentro está dotado de una pequeña alarma que incluye: panel de control, sirena externa, sensores de movimiento, sensores magnéticos, sensor de humo, y botón de pánico, sin embargo el tema de la seguridad es algo que preocupa debido a que los equipos que son parte del Infocentro pueden ser blanco de la delincuencia ya que algunos Infocentros se encuentran totalmente alejados de las Unidades de Vigilancia Comunitaria.

Con el planteamiento de estos dos problemas se propone el "Diseño de una red VPN para la integración de los servicios de VoIP y video vigilancia para los Infocentros comunitarios", con estos dos servicios se solucionará en gran medida los problemas de comunicación entre los Infocentros, ya que al contar con una red de VoIP, se dotará a los facilitadores y al equipo de trabajo del Proyecto Ampliación de la Red Infocentros de una herramienta de comunicación, que resultará mucho más ágil, ya que el facilitador puede reportar de manera inmediata cualquier novedad suscitada en el día y a su vez gestores sociales y coordinadores zonales pueden mantener un control constante de cualquier Infocentro que se encuentre dentro de la red de VoIP.

En el diseño de esta red se contempla el uso de video cámaras digitales, que puedan monitorear lo que se encuentra sucediendo al interior del Infocentro, de esta manera controlar la atención

del Facilitador y a su vez de proveer de una herramienta que ayude con la seguridad del Infocentro.

3. ANTECEDENTES

Los Infocentros comunitarios han sido implementados y desarrollados por otros países en América, Asia y África, conocidos bajo la denominación de Telecentros.

En África encontramos 2 modelos de telecentro bien diferenciados, los telecentros comerciales y los comunitarios, los primeros están gestionados por pequeños empresarios e impulsados en su mayoría por los gobiernos y los operadores de telecomunicación y su objetivo es el extender el acceso universal a la telefonía. Por el contrario, los telecentros comunitarios están financiados en su mayor parte por instituciones internacionales y gestionados por las propias comunidades, su objetivo es proporcionar acceso a las TIC a las comunidades del África rural para fortalecer y vertebrar su proceso de desarrollo. [20]

América es con diferencia el continente que presenta una mayor diversidad de modelos de telecentro, se las puede dividir en función del tipo de organización que las haya iniciado: las de iniciativa privada (pequeños empresarios u operadores de telecomunicación), aquellas cuya instalación ha partido de organizaciones sociales (como ONG, organizaciones comunitarias de base u organismos multilaterales de cooperación) y por último las de iniciativa pública, que forman parte de un programa gubernamental de desarrollo de telecentros. [20]

En Asia ha prevalecido el desarrollo de los telecentros comerciales, existiendo numerosas franquicias y operadores de telecomunicación que los apoyan. Sin embargo, el número de experiencias de telecentros comunitarios es comparativamente muy inferior a los de África y América. [20]

Desde el año 2001 el gobierno venezolano inició un Plan masivo de acceso a Internet con el fin de facilitar la incorporación al uso de estas tecnologías por sectores de la población, tradicionalmente excluidos. Mediante el decreto 825, se puso en marcha el programa Infocentros a nivel nacional, el desarrollo del Plan se sustenta en la Constitución y en el Plan

Nacional de Telecomunicaciones, donde se reconoce el interés público, por la ciencia, la tecnología, el conocimiento y los servicios de información, a través de la inserción de las instituciones educativas venezolanas dentro del concepto de la sociedad de la información y del conocimiento, por medio de la incorporación de las mismas al uso y aplicación de las diferentes alternativas disponibles en Internet.[19]

4. OBJETIVOS:

4.1. OBJETIVO GENERAL

Diseñar una red VPN para la integración de los servicios de VoIP y video vigilancia para los Infocentros Comunitarios del proyecto Ampliación de la Red Infocentros.

4.2. OBJETIVOS ESPECÍFICOS:

1. Análisis de la situación actual del proyecto Infocentros y de los servicios que se prestan a la ciudadanía.
2. Seleccionar los equipos necesarios para el servicio de VoIP y video vigilancia.
3. Diseño de la topología de la red VPN, para el intercambio de voz, video y datos entre los Infocentros Comunitarios.
4. Dimensionamiento del ancho de banda requerido para la integración de estos servicios.
5. Análisis de las políticas de QoS sobre la red diseñada.

5. DESARROLLO DEL CASO DE ESTUDIO

5.1. ANÁLISIS DE LA SITUACIÓN ACTUAL DEL PROYECTO INFOCENTROS Y DE LOS SERVICIOS QUE SE PRESTAN A LA CIUDADANÍA.

5.1.1. Marco Legal

La Constitución de la República del Ecuador, en su capítulo Segundo Derechos del Buen Vivir, sección tercera Comunicación e Información, establece que:

"Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. *Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos.*
2. *El acceso universal a las tecnologías de información y comunicación. "*

"Art. 17.- El Estado fomentará la pluralidad y la diversidad en la comunicación, y al efecto: (…)

2. Facilitará la creación y el fortalecimiento de medios de comunicación públicos, privados y comunitarios, así como el acceso universal a las tecnologías de información y comunicación en especial para las personas y colectividades que carezcan de dicho acceso o lo tengan de forma limitada."[1]

El Plan Nacional del Buen Vivir 2013-2017, aprobado por el Concejo Nacional de Planificación indica dentro de sus objetivos:

"Objetivo 4.- Fortalecer las capacidades y potencialidades de la ciudadanía.

- *Política 4.3. Promover espacios no formales y de educación permanente para el intercambio de conocimientos y saberes para la sociedad aprendiente.*

  a) Democratizar el acceso al conocimiento, fortaleciendo los acervos de datos, la información científica y los saberes diversos en todos sus formatos, desde espacios físicos y virtuales de libre acceso, reproducción y circulación en red, que favorezcan el aprendizaje y el intercambio de conocimientos.
- *Política 4.4. Mejorar la calidad de la educación en todos sus niveles y modalidades, para la generación de conocimiento y la formación integral de personas creativas, solidarias, responsables, críticas, participativas y productivas, bajo los principios de igualdad, equidad social y territorialidad.*

  j) Crear y fortalecer infraestructura, equipamiento y tecnologías que, junto al talento humano capacitado, promuevan el desarrollo de las capacidades creativas, cognitivas y de innovación a lo largo de la educación, en todos los niveles, con criterios de inclusión y pertinencia cultural.
- *Política 4.6. Promover la interacción recíproca entre la educación, el sector productivo y la investigación científica y tecnológica, para la transformación de la matriz productiva y la satisfacción de necesidades.*

  a) Generar oferta educativa e impulsar la formación de talento humano para la innovación social, la investigación básica y aplicada en áreas de producción priorizadas, así como la resolución de problemas nacionales, incentivando la articulación de redes de investigación e innovación con criterios de aprendizaje incluyente."[3]

El MINTEL cuenta con su Planificación Estratégica Institucional para el año 2016, en sus políticas establece:

- *"Propiciar el desarrollo social, solidario e inclusivo en sectores rurales, urbano marginales, comunidades y grupos de atención prioritaria, a través del uso intensivo de TIC.*
- *Acercar la administración del Estado y sus procesos a la ciudadanía y a los sectores productivos, proveyendo servicios de calidad, accesibles, seguros, transparentes y oportunos, a través del uso intensivo de las TIC.*
- *Convertir a las TIC en uno de los ejes de transformación productiva y desarrollo económico."*

Sus objetivos estratégico Institucionales son:

- *"Incrementar el número de ciudadanos incluidos digitalmente*
- *Incrementar el uso de las TICs en el ámbito público, privado y la sociedad en general."[4]*

5.1.2. Definición de Infocentro

Los Infocentros son espacios comunitarios de participación y desarrollo, que garantizan el acceso inclusivo a las Tecnologías de la Información y Comunicación de las poblaciones de parroquias rurales y urbanas marginales del Ecuador.

El proyecto contempla la implementación y operación de 808 Infocentros comunitarios y 25 Megainfocentros, en parroquias rurales, urbano marginales, el objetivo es dotar de herramientas a la población de las zonas rurales y urbanas marginales para que puedan capacitarse en temas de uso de las Tecnologías de la Información y Conocimiento, los elementos que componen un Infocentro son: Equipamiento, conectividad, recurso humano.

Equipamiento.- en cuanto a su equipamiento se consideran dos tipos: Infocentros y Megainfocentros, estos han sido ubicados en cada población en su mayoría evaluando el índice poblacional, un Infocentro está compuesto de los siguientes equipos: [5]

- 1 servidor Infocentro
- 10 thin-client
- 11 monitores

- 1 proyector
- 1 impresora multifunción sistema de tinta continua
- 1 switch de rack Infocentro
- 1 regulador principal
- 10 reguladores de voltaje para thin client
- 1 sistema de alarma
- 1 video cámara digital
- 1 aire acondicionado
- 1 televisor 42”
- Cableado estructurado y accesorios
- Cableado eléctrico y accesorios
- Servicio de Internet
- Servicio de Televisión Satelital DTH
- Mobiliario
- Señalética

Un Megainfocentro está compuesto de los mismos equipos, pero estos difieren en cantidad:

- 1 servidor Megainfocentro
- 50 Thin-client
- 51 monitores
- 3 proyectores
- 1 impresora multifunción sistema de tinta continua
- 1 switch de rack Megainfocentro
- 1 regulador principal
- 50 reguladores de voltaje para thin client
- 1 sistema de alarma
- 1 video cámara digital
- 2 aire acondicionado
- 2 televisor 42”
- Cableado estructurado y accesorios
- Cableado eléctrico y accesorios
- Servicio de Internet
- Servicio de Televisión Satelital DTH

- Mobiliario
- Señalética

Recurso Humano.- La atención del Infocentro se la realiza a través de:

- Facilitador, que es la que se encarga de administrar, operar y controlar el Infocentro bajo directriz del MINTEL en coordinación de los Gestores Sociales.
- Gestor Social. Realiza labores de inclusión social del Infocentro en la comunidad, bajo directriz del MINTEL.

Para la labor de estos actores, se asegura la provisión del servicio de conectividad, durante la vigencia de operatividad de los Infocentros.

Conectividad.- la tecnología usada para la dotación de este servicio se resume en la Tabla 5.1:

Tabla 5. 1 Detalle de conectividad de los Infocentros y Megainfocentros

CONECTIVIDAD INFOCENTROS		
TECNOLOGÍA	***COMPARTICIÓN***	***VELOCIDAD***
ADSL	*2:1*	*2048 kbps x 768 kbps*
FIBRA ÓPTICA	*2:1*	*4000 kbps x 2048 kbps* *2048 kbps x 2048 kbps*
VSAT	*4:1*	*1024 kbps x 512 kbps*
CONECTIVIDAD MEGAINFOCENTROS		
FIBRA ÓPTICA	*1:1*	*10 Mbps x 10 Mbps*

Tres tipos de tecnologías son utilizadas para proporcionar el servicio de Internet a los Infocentros: ADSL, Fibra Óptica, VSAT; esto depende de la situación geográfica en donde se encuentran ubicados los Infocentros, en su mayoría están dotados del servicio de internet a través de ADSL, la Fibra Óptica es utilizada para el caso de Megainfocentros por el requerimiento de mayor ancho de banda o para Infocentros que se localizan en zonas urbano marginales, VSAT es utilizada para los casos en los que un Infocentro se encuentra situado en una localidad en la que no existe líneas ADSL y que por la irregularidad de la zona se imposibilita la instalación de cableado y postería, o a su vez la instalación de estos es demasiado costoso y no representa una buena inversión para la empresa dotadora de este servicio.

La Tabla 5.2 detalla el número de Infocentros de acuerdo a la tecnología utilizada para dotar del servicio de conectividad.

Tabla 5. 2 Número de Infocentros/Megainfocentros por tecnología

TECNOLOGÍA	CANTIDAD	DENOMINACIÓN
ADSL	122	Infocentros
	0	Megainfocentros
FIBRA ÓPTICA	50	Infocentros
	24	Megainfocentros
VSAT KU	122	Infocentros
	0	Megainfocentros

Debido a la velocidad y el nivel de compartición que ofrece la tecnología VSAT KU y ADSL, los Infocentros que se encuentran con esta tecnología no serán considerados dentro de este estudio.

El enlace de Fibra Óptica conecta con la red interna del Infocentro por medio de un equipo CISCO 881-K9, con las siguientes características:

- Cuatro puertos 10/100 Fast Ethernet con soporte VLAN ; dos puertos son compatibles con alimentación a través de Ethernet (PoE) para la alimentación de los teléfonos IP o puntos de acceso externos
- Seguridad 802.11g / n basada en el proyecto de norma 802.11n con soporte para arquitecturas WLAN unificada autónomas o Cisco
- Un puerto USB 1.1 para las credenciales de seguridad eToken , el arranque desde USB , y la configuración de carga
- Fácil configuración , implementación y de administración remota capacidades a través de herramientas basadas en la web y el software Cisco IOS
- Firewall
- Filtrado de contenido
- VPN y WLAN , a velocidades de banda ancha para pequeñas oficinas
- Un plus de seguridad avanzada, incluyendo la prevención de intrusiones , GET VPN , VPN dinámica multipunto (DMVPN) para un máximo de 20 de sitio a sitio de túneles VPN
- Cisco Configuration Professional para una gestión simplificada
- Conexión WAN con múltiples opciones de acceso

En la Fig. 5.1 muestra las interfaces físicas del equipo CISCO 881-K9.

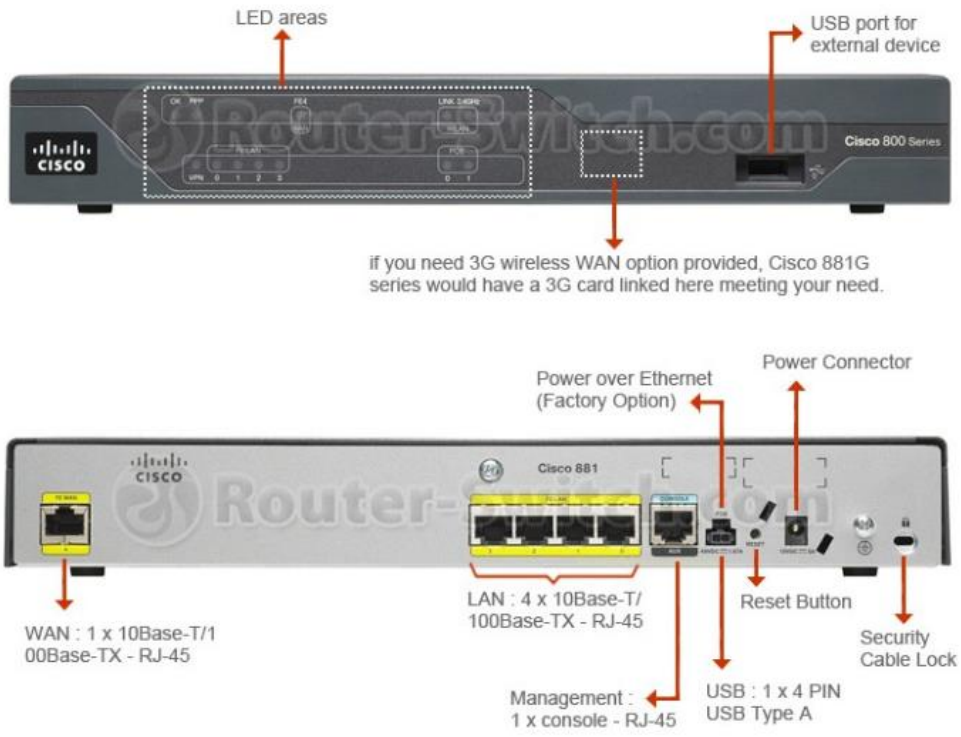


Fig 5. 1 Router CISCO 881-K9

Este equipo será aprovechado para la configuración de los servicios de telefonía y video vigilancia sobre una red VPN, es por ello que se considera para este estudio solo los Infocentros que disponen de enlaces de Internet a través de fibra óptica; el detalle del número de Infocentros por tipo de conectividad fue mencionado en la Tabla 5.2.

Por lo expuesto se realiza el dimensionado del equipamiento para los sistemas de telefonía y video vigilancia IP para un total de 50 Infocentros y 24 Megainfocentros con tecnología de fibra óptica para el acceso a Internet.

5.1.3. Localización

Ecuador es un país conformado por cuatro regiones: Costa, Sierra, Oriente y Región Insular. Actualmente dividida en 24 provincias, el proyecto Ampliación de la Red Infocentros tiene como objeto la implementación y operatividad de 267 Infocentros y 24 Megainfocentros que se sitúan en las diferentes de provincias del Ecuador, en la Tabla 5.3 se encuentra la distribución de los Infocentros por provincia.

Tabla 5. 3 Distribución de Infocentros y Megainfocentros por provincia

PROVINCIA	# INFOCENTROS	# MEGAINFOCENTROS
AZUAY	3	1
BOLIVAR	5	0
CAÑAR	4	1
CARCHI	20	2
CHIMBORAZO	26	3
COTOPAXI	16	1
EL ORO	16	0
ESMERALDAS	17	1
GUAYAS	32	1
IMBABURA	4	1
LOJA	17	1
LOS RIOS	5	2
MANABÍ	26	3
MORONA SANTIAGO	1	1
NAPO	1	0
PASTAZA	2	0
PICHINCHA	23	2
SANTA ELENA	11	0
SANTO DOMINGO DE LOS TSÁCHILAS	16	1
SUCUMBIOS	3	0
TUNGURAHUA	19	3

5.1.4. Servicios que ofrece un Infocentro

Dentro de los servicios que se brinda en un Infocentro a la comunidad, es el acceso gratuito a internet, investigaciones, correo electrónico, redes sociales, información y servicio de las entidades de gobierno y capacitaciones en temas de alistamiento digital.

De acuerdo a las políticas del MINTEL, mensualmente se debe contar con un total de 20 personas capacitadas para Infocentros y 50 personas capacitadas para Megainfocentros, los contenidos de

las capacitaciones son preparadas y supervisadas por la Dirección de Alistamiento Digital del MINTEL, las temáticas son las siguientes:

- Fundamentos de Operación Básica del Computador
- Optimizando los Recursos Informáticos Disponibles
- Tecnologías de la Información para la Productividad
- Formación de Formadores de los Infocentros
- Diseño de páginas Web Comunitarias
- Ensamblaje y Mantenimiento de Computadoras
- Formador de Formadores
- Micro emprendimiento con TIC.
- Introducción a las TIC
- Herramientas de Gobierno Electrónico
- Herramientas Ofimáticas
- TIC Emprendimiento
- Redes Sociales como herramientas de Comunicación
- Redes Sociales para jóvenes
- TIC Artesanos
- TIC Negocios para Mi Pymes
- TIC Turismo

5.1.5. Arquitectura de Red de un Infocentro

La Fig 5.2 muestra la arquitectura de un Infocentro y la Fig 5.3 la arquitectura de un Megainfocentro con tecnología Fibra óptica, en la Tabla 5.4, se encuentran en detalle las especificaciones técnicas de los Equipos que se encuentran instalados en un Infocentro y Megainfocentro.

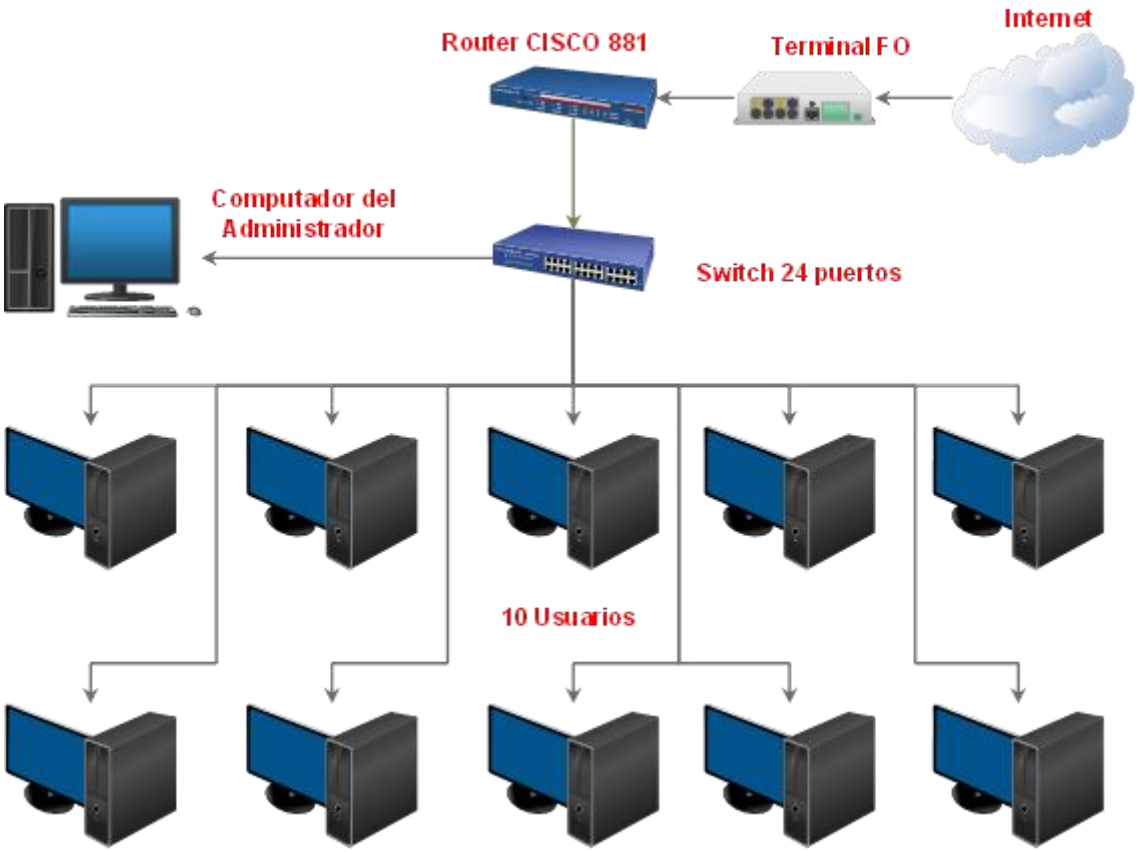


Fig 5. 2 Arquitectura de red de un infocentro

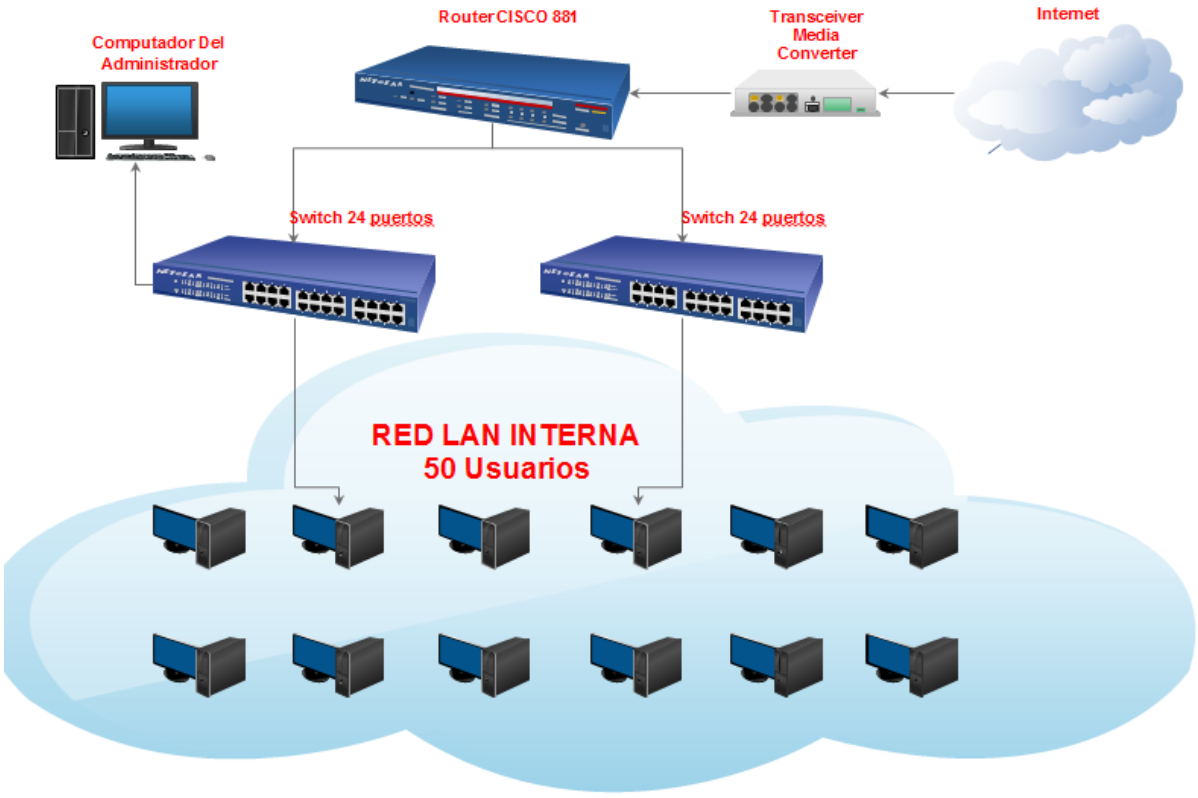


Fig 5. 3 Arquitectura de red de un Megainfocentro

Tabla 5. 4 Especificaciones técnicas de los equipos de un Infocentro

SERVIDOR		COMPUTADORES USUARIOS / THIN CLIENT	
Marca – modelo	INTEL – DH87RL	Procesador	INTEL CELERON
Número de canales de memoria	4	Resoluciones de pantalla soportados	1280 x 800., 24 bits de color
Número de procesadores	1	Método de Conexión al Servidor	Ethernet
Núcleos	4/cada procesador	Conector de Red	RJ-45
Velocidad	3300 MHZ	Conexión a red	Ethernet 10/100 Mbps
Memoria caché	8 MB	Video	Acelerador o tarjeta gráfica de video
Memoria Instalada	16 GB DDR3	Puertos USB	4 Puertos USB ,
CONTROLADOR DE RED			
Velocidad	Gigabit Ethernet 10/100/1000 Mbps		
Puerto Ethernet RJ-45	RJ-45 (10Base-T/100Base-T/1000Base-T)		
Estándar	IEEE 802.3		
Velocidad	Gigabit Ethernet 10/100/1000 Mbps		
ALMACENAMIENTO			
Cantidad de Discos Duros:	2 Discos		
Capacidad	1 TB (por cada disco duro)		
Velocidad	15000 RPM		
Interfaz	SAS o SATA		

5.1.6. Operatividad del Infocentro

Para que un Infocentro se encuentre operativo, el mismo debe cumplir con lo siguiente:

- Implementación del Equipamiento, Mobiliario y Señalética
- Instalación de los servicios de Internet, DTH, y filtrado de páginas Web.
- Contratación de un facilitador por Infocentro y dos facilitadores para un Megainfocentro.

El Gestor Social es la persona que se encarga en cada provincia de llevar un control de la operatividad de cada Infocentro y reportar las novedades encontradas a los coordinadores que se encuentran en el MINTEL, sin embargo esta se convierte en una tarea exhaustiva tomando en cuenta que los gestores sociales deben hacer visita en sitio y los Infocentros se encuentran en zonas rurales, lo que ha llevado a las siguientes situaciones.

- Los Facilitadores reportan su asistencia a su jornada laboral a través de mails, o a su vez se realiza un registro físico que es firmado por el presidente del GAD parroquial.
- Los Coordinadores pueden comunicarse a con los Facilitadores vía celular o a través de las redes sociales, esto hace vulnerable el control que se realiza al trabajo del facilitador.

5.1.7. Requerimientos de Servicio

De acuerdo a lo expuesto anteriormente, se plantea la dotación de los siguientes servicios:

- Conectividad para todas las estaciones de trabajo del Infocentro.
- Para ofrecer una mayor seguridad para los usuarios de los Infocentros, así como también del personal que aquí labora y del equipamiento que en él se encuentran, se prevé la implementación de una cámara de vigilancia.
- Para mejorar la comunicación entre los facilitadores y el personal que control de la operatividad de los Infocentros, se prevé la instalación de un sistema de telefonía IP.
- Debido a que los Infocentros no se encuentran bajo la misma infraestructura de red, será necesario la creación de una VPN cuya central serán las oficinas del Ministerio de Telecomunicaciones en la ciudad de quito, de modo que los Infocentros puedan comunicarse como accesos remotos y hagan uso de los servicios que la red ofrece.

5.2. SELECCIONAR LOS EQUIPOS NECESARIOS PARA EL SERVICIO DE VOIP Y VIDEO VIGILANCIA.

5.2.1. Servicio de Video Vigilancia IP

En la actualidad los sistemas de video vigilancia han evolucionado del sistema de circuito cerrado de televisión (CCTV), al sistema de video vigilancia IP y con esto se ha logrado un gran salto en las funcionalidades y la accesibilidad que ofrece la tecnología IP, en comparación con su antecesora.

CCTV.- Un sistema de circuito cerrado de TV completamente analógico está compuesto por: cámaras analógicas con salida coaxial, VCR (grabador de video) y un monitor analógico para visualizar el video, en la Fig 5.4 muestra un sistema de video vigilancia totalmente analógico, uno de las deficiencias de los sistemas analógicos es que el video no se comprime, por lo que al grabar a una velocidad de imagen completa, la cinta de video durará un máximo de 8 horas. [W13]

Existen sistemas híbridos, en los que un servidor de video permite la incorporación de cámaras de video analógicas a una red IP, para lo cual el servidor de video será el encargado de digitalizar la imagen antes de poder transmitirla. [8]

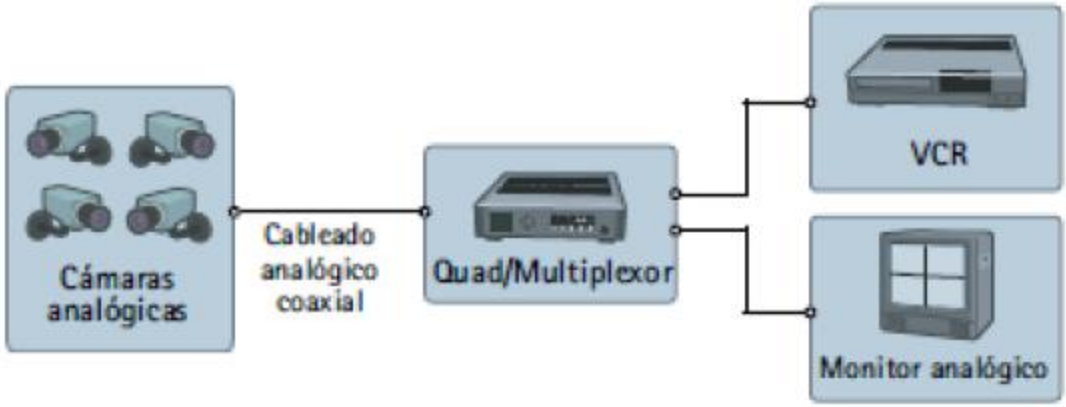


Fig 5. 4 Sistema de video vigilancia analógico

Algunas de las ventajas que posee el sistema de video vigilancia IP, frente a la tecnología analógica, son las siguientes:

- Cámaras de alta resolución (megapíxel)
- Calidad de imagen constante
- Alimentación eléctrica a través de Ethernet y funcionalidad inalámbrica

- Funciones de Pan/tilt/zoom, audio, entradas y salidas digitales a través de IP, junto con el vídeo
- Flexibilidad y escalabilidad completas

5.2.1.1. Elementos de un Sistema de Video IP

Una de las características principales del video IP es que no necesita un cableado punto a punto dedicado, ya que utiliza la misma red como eje central para su servicio y pueden ser grabados o monitoreados desde cualquier parte del mundo en donde exista una conexión a internet y verlos en tiempo real, los principales elementos para un sistema de video IP, son los siguientes:

- Cámara IP.- es el dispositivo que capta las imágenes y las transmite a través de una red IP, de este modo los usuarios habilitados pueden visualizar, almacenar o gestionar las imágenes de acuerdo al requerimiento, una cámara IP no necesita estar conectada a un computador para su funcionamiento, basta con que se la conecte a un punto de acceso a la red IP.
- Servidor de video.- un servidor de video permite incorporar la tecnología analógica a una red IP, dispone de puertos para la conexión con cámaras analógicas, dispone de una función de compresión de video, un sistema de video IP puro puede prescindir de este componente debido a que el video puede grabarse de manera directa en un computador estándar.
- Software de gestión de video.- El software de video puede trabajar en Linux o Windows de acuerdo a las características del servidor de video, usualmente utiliza una interfaz Web, ofrece las funciones de visualización simultánea, diferentes modos de grabación (continua, programada o por alarmas), la Fig 5.5 muestra un ejemplo de software de gestión de video. [6]

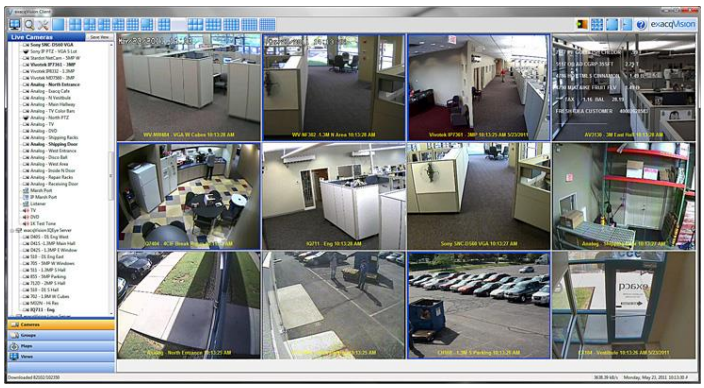


Fig 5. 5 Software de Sistema de Gestión de Video

5.2.1.2. Estándares de compresión de video

JPEG – Motion (M-JPEG).- Vídeo como una secuencia de imágenes JPEG, es el estándar utilizado más habitualmente en sistemas de vídeo IP, debido a su nivel de compresión. Una cámara de red, como una cámara digital de imagen fija, capta las imágenes individuales y las comprime en formato JPEG. La cámara IP puede captar y comprimir, las dispone en una secuencia continua de imágenes a través de una red hasta una estación de visualización. [W14]

H.263.- fue diseñado para aplicaciones de videoconferencia, la técnica de compresión H.263 se encarga de una transmisión de vídeo con una tasa de bits fija. La desventaja de tener una tasa de bits fija es que cuando un objeto se mueve, la calidad de la imagen disminuye. [20]

MPEG.- el principio básico de MPEG es la comparación de dos imágenes comprimidas que deben transmitirse a través de la red, la primera imagen comprimida se utiliza como fotograma de referencia y únicamente se envían partes de las siguientes imágenes que son distintas de la imagen de referencia, posterior a esto la estación de monitoreo o visualización de red reconstruye todas las imágenes basándose en la imagen de referencia y los datos de diferencias. Existen diversos estándares MPEG diferentes:

- MPEG-1.- su objetivo era el almacenamiento de vídeo digital en CD. Por tanto, la mayoría de codificadores y descodificadores MPEG-1 están diseñados para una tasa de bits de destino de aproximadamente 1,5Mbit/s, con resolución CIF.
- MPEG-2.- fue diseñado para vídeo digital de alta calidad (DVD), TV digital de alta definición (HDTV), soportes de almacenamiento de datos (ISM), vídeo de difusión digital (DBV) y TV por cable (CATV).
- MPEG-4 es la evolución de MPEG-2, tiene varias herramientas para reducir la tasa de bits manteniendo la calidad de la imagen, este estándar de compresión soporta un factor de compresión que está en el rango de 70:1 para movimiento y 200:1 para imágenes estáticas, se pueden usar factores de compresión dentro de este rango y su elección estará basada en el número de imágenes por segundo que se utilizará en la configuración del sistema de video.

La consideración clave es seleccionar un estándar de compresión de vídeo ampliamente usado para asegurar una calidad de imagen elevada, tales como MJPEG y MPEG-4, el consumo de ancho

de banda es un parámetro determinante a la hora de elegir un estándar de compresión de video, si el ancho de banda de red disponible se encuentra limitado o si el vídeo debe grabarse a una velocidad de imagen elevada y existen limitaciones en el espacio de almacenamiento, MPEG puede ser la opción más adecuada. Ofrece una calidad de imagen relativamente elevada a una tasa de bits inferior, la Fig 5.6 muestra cómo se compara el uso de ancho de banda entre Motion JPEG y MPEG-4 en una determinada escena de imágenes con movimiento. [W14]

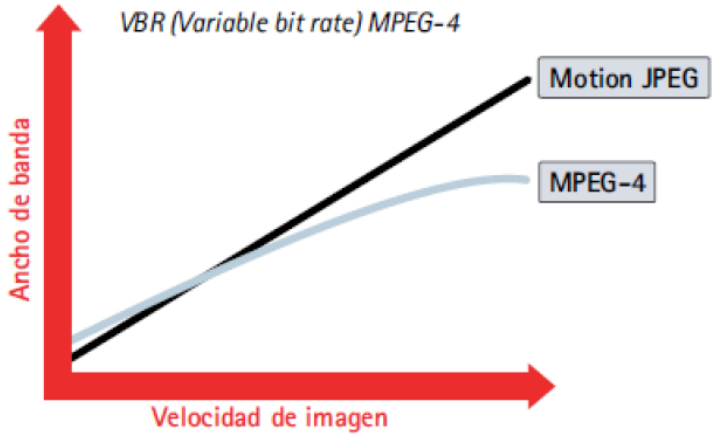


Fig 5. 6 Comparación del uso del ancho de banda de acuerdo al estándar

5.2.1.3. Resolución de video

- Resoluciones NTSC y PAL.- En América del Norte y Japón, el estándar NTSC (Comité Nacional de Sistemas de Televisión) es el estándar de vídeo analógico predominante, mientras que en Europa se usa el estándar PAL (Línea de Alternancia de Fase). Ambos estándares proceden de la industria de la televisión. NTSC tiene una resolución de 480 líneas horizontales y una velocidad de renovación de 60 campos entrelazados por segundo (o 30 imágenes completas por segundo). PAL tiene una resolución de 576 líneas horizontales y una velocidad de renovación de 50 campos entrelazados por segundo (o 25 imágenes completas por segundo). La cantidad total de información por segundo es la misma en ambos estándares. [W15]
- Resolución VGA.- Video Graphics Array (Tabla de Gráficos de Vídeo), un sistema de exposición gráficos para PC, la resolución se define a 640x480 píxels, un tamaño muy parecido a NTSC y PAL. La resolución VGA es normalmente más adecuada para las cámaras IP, ya que el vídeo en la mayoría de los casos se mostrará en pantallas de ordenador, con resoluciones en VGA o múltiplos de VGA. [W15]
- MPEG.- La resolución MPEG normalmente significa una de las resoluciones siguientes:

- 704x576 pixels (PAL 4CIF)
- 704x480 pixels (NTSC 4CIF)
- 720x576 píxels (PAL o D1)
- 720x480 píxels (NTSC o D1)

- Resolución Megapíxel.- Un formato megapíxel común es 1.280x1.024, que ofrece una resolución de 1,3 megapíxeles, 3 veces más que en las cámaras analógicas. Las cámaras con 2 megapíxels y 3 megapíxels también se encuentran disponibles. [W15]

5.2.1.4. Selección de la Cámara IP

En la Tabla 5.5 se muestra la cámara IP seleccionada y sus características. [W1]

Tabla 5. 5 Características de la cámara IP seleccionada

CÁMARA DOMO IP, DS-2CD793PF-E.		
CARACTERÍSTICAS TÉCNICAS:		
Sensor	CCD 1/3”	
Resolución	4CIF	
Conmutación	Día/Noche electrónica	
Alimentación	12VDC- 375mA o PoE	
Lux min	0,02lux	
E/S	Audio, Alarma	
Compresión	H.264, MPEG4, MPEG	
Servidor Web	integrado	
Acepta tarjeta SD	Max 32GB	
Salida de video	(Ethernet 10/100Mbps)	
Número de frames por segundo	25fps	

5.2.1.5. Protocolos para la transmisión de video IP

La transmisión de video está encargada al conjunto de protocolos TCP/IP.

Tabla 5. 6 Protocolos para la transmisión de video IP.

PROTOCOLO	**PROTOCOLO DE TRANSPORTE**	**PUERTO**	**USO COMÚN**	**USO VÍDEO EN RED**

FTP File Transfer Protocol	TCP	21	Transferencia de ficheros a través de Internet/intranets	Transferencia de imágenes o vídeo desde una cámara de red o servidor de vídeo a un servidor FTP o a una aplicación
SMTP Send Mail Transfer Protocol	TCP	25	Protocolo para el envío de e-mails	Una cámara de red o servidor de vídeo puede enviar imágenes o notificaciones de alarma utilizando su cliente integrado de e-mail
HTTP Hyper Text Transfer Protocol	TCP	80	Utilizado para navegar en la web, p.e. para recibir páginas web de servidores web	El modo más común de transferencia de vídeo desde una cámara de red o servidor de vídeo donde el dispositivo trabaja como un servidor web, proporcionando vídeo al usuario o servidor de aplicación
HTTPS Hypertext Transfer Protocol over Secure Socket Layer	TCP	443	Utilizado para acceder a páginas web de forma segura utilizando encriptación	La transmisión de vídeo desde una cámara de red o servidor de vídeo puede ser utilizada para autenticar los envíos de la cámara utilizando certificados digitales X.509
RTP Real Time Protocol	UDP/TCP	No definido	Formato de paquetes estandarizado RTP para el envío de vídeo y audio a través de Internet. A menudo utilizado en sistemas multi-media o de	Un modo común de transmitir vídeo en red MPEG La transmisión puede ser unicast (uno a uno) o multicast (uno a varios)

			video conferencia	
RTSP Real Time Streaming Protocol	TCP	554	Utilizado para configurar y controlar sesiones multimedia a través de RTP	

5.2.1.6. Tipos de almacenamiento

Las unidades de almacenamiento de un sistema IP se utilizan para monitorizar, grabar, administrar y archivar secuencias de video, pueden ser de tres tipos:

Almacenamiento en el mismo dispositivo.- Las cámaras IP poseen una memoria interna con un tamaño de almacenamiento limitado, usado para casos en los que el almacenamiento es crítico o no puede enviarse a través de la res y la grabación no puede interrumpirse. [7]

Almacenamiento en el mismo PC en el que se instale el software de control.- se lo utiliza para instalaciones pequeñas. La cantidad de memoria disponible viene determinada por las características del disco duro del computador.

Almacenamiento en NVR (Network Video Recorder).- es útil para instalaciones profesionales, el soporte de grabación es generalmente un disco duro de grandes capacidades, se puede conectar al NVR un monitor LCD para visualizar las grabaciones, y un teclado especial para controlar el movimiento y/o zooms desde el propio grabador. El NVR puede conectarse en cualquier parte de la LAN, solo requiere una conexión a internet con IP fija, para casos en los que se requiera almacenar una gran cantidad de información se puede conectar varios NVR a la red, existen además varios métodos de grabación: [7]

- Grabación continúa.- el grabador está grabando durante todo el tiempo.
- Grabación programada.- sólo se graba en ciertos periodos (hora/día/semana) programados.
- Grabación por eventos. El grabador únicamente graba en los momentos de detección de movimiento o de disparo de alarma.
- Grabación por eventos y por tiempo. La grabación se realiza cuando se produce algún evento, pero únicamente dentro de unos horarios establecidos.

Revisados los métodos de almacenamiento del video, se elige la instalación de un equipo NVR cuyo dimensionamiento se lo realizará posteriormente.

5.2.1.7. Software de gestión y control de video

Aunque el vídeo puede visualizarse directamente desde un navegador Web estándar, puede instalarse el software de gestión de vídeo si se requieren tener más opciones de visualización, cada NVR dispone de software de gestión de video, cuyas funciones son:

- Programación de los modos de grabación: grabación local, grabación remota, grabación manual, grabación programada.
- Visualización de las grabaciones
- Configuración de los dispositivos
- Programación de alarmas, registro de eventos y parámetros de arranque.

5.2.2. Servicio de VoIP

Voz sobre Protocolo de Internet, también llamado Voz sobre IP, Voz IP, VoIP, son un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Protocolo de Internet), convirtiendo a la señal de voz en forma digital en paquetes de datos, en lugar de enviarla en forma analógica a través de circuitos utilizables como en la telefonía convencional, algunos de los beneficios de la Telefonía IP son: [W2]

- Interoperabilidad con las redes telefónicas actuales
- Calidad de Servicio
- Red de alta disponibilidad
- Calidad de voz garantizada
- Reducción de costos
- Facilita creación de extensiones telefónicas adicionales
- Telefonía IP ayuda a mejorar la comunicación
- La comunicación unificada permite trabajar de forma remota desde cualquier lugar con una conexión a Internet.
- Telefonía IP permite disfrutar de muchas funciones: buzón de voz, ID de llamada, conferencias, entre otras.

5.2.2.1. Telefonía tradicional

Al principio, para que un abonado se comunicara con otro este debía solicitar la llamada a una operadora, quien manualmente conectaba los cables para conmutar un punto con otro. En 1891 se inventó un teléfono automático, que permitía marcar directamente, para finales de la segunda guerra mundial el servicio telefónico llegaba a millones de abonados; la telefonía analógica ha venido funcionando por mas de 100 años, a través de un sistema de conmutación de circuitos. En este sistema cuando una llamada es realizada la conexión es mantenida durante todo el tiempo que dure la comunicación. [10]

Fig 5. 7 Telefonía tradicional

5.2.2.2. Protocolos de VoIP

Los protocolos VoIP definen la manera en que los CODECS de audio se conectan entre si y hacia otras redes usando VoIP.

PROTOCOLO H.323

Establecida por la ITU, fue el primer protocolo elaborado para la transmisión de contenido multimedia (voz, video, sonidos, etc). El estándar contempla el control de la llamada, gestión de la información y ancho de banda para una comunicación punto a punto y multipunto.

Características principales de H.323: [12]

- Es el estándar más completo para transmisiones de voz y video
- La calidad de servicio también es mayor ya que se ocupa de este tema en cada uno de sus protocolos que componen el estándar.
- Está orientado a la comunicación de dispositivos multimedia dentro de una red LAN, con la posibilidad de interactuar con la PSTN o ISDN

- Es posible transmitir voz, datos, video.
- Este protocolo funciona sobre varias topologías de red y el software requerido para que el protocolo funcione de manera obligatoria es el software de voz, mientras que el software orientado a la transmisión de datos y video es opcional.
- Necesita de otros protocolos y equipos que gestión en la comunicación entre los diferentes dispositivos y redes de telefonía.
- Interoperabilidad entre distintos fabricantes.
- Independencia de la plataforma y de la aplicación. Siempre que se cumplan los requisitos y procedimientos descritos en las especificaciones, podrá hacer uso de H.323 cualquier plataforma, hardware o sistema operativo deseado.
- Soporte para multi conferencias.
- Gestión del ancho de banda.- permite la gestión del ancho de banda, limitando el número de conexiones H.323 simultáneas.
- Soporte para el establecimiento de conferencias entre distintas redes multimedia.- establece mecanismos para unir sistemas basados en comunicaciones LAN con sistemas RDSI, así como con las redes PSTN, tanto en audio como en videoconferencias.
- Intercambio de requerimiento de calidad de servicio.- un destino puede especificar una calidad de servicio deseada para sus flujos de audio y vídeo
- Gestión del direccionamiento entre dominios administrativos.- se establecen mecanismos de escalado para el establecimiento de llamadas entre grandes redes internacionales.

Arquitectura del protocolo H.323

Los equipos que intervienen en su arquitectura, se los identifica en la Fig. 5.8:

- Equipos Terminales
- Gateways para su interconexión con los recursos PSTN
- Gatekeepers para el (Control de admisión, registro y ancho de banda)
- MCUs (Multiconference Control Units)

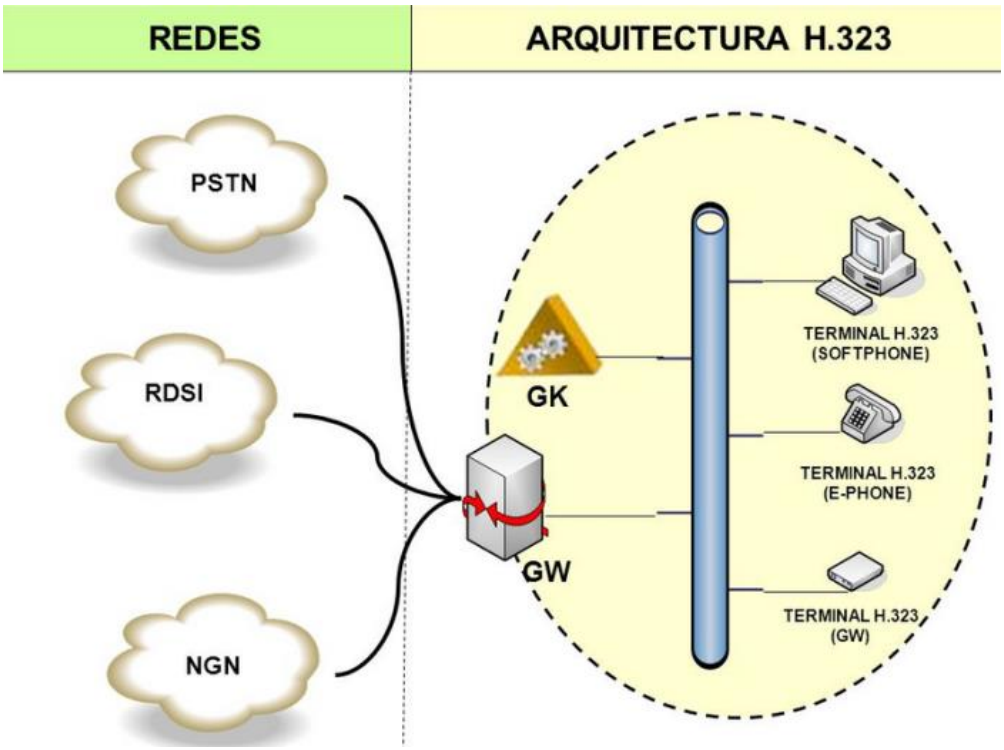


Fig 5. 8 Arquitectura H.323

PROTOCOLO SIP

Session Initiation Protocol (SIP).- es un protocolo estandarizado por la IETF, utilizado para establecer, mantener y terminar sesiones multimedia. El protocolo SIP se compone de agentes de usuarios y servidores de red (clientes y servidores). SIP es un protocolo flexible que tiene posibilidades de extensión para funciones y servicios adicionales. La arquitectura de SIP es modular, solo cubre la señalización básica, la localización de usuarios y el registro, otras características se implementan en protocolos separados. La base de su desarrollo fueron protocolos de aplicación de redes de datos como HTTP y SNMP. [21]

Ventajas

- Tiene mayor simplicidad, utiliza mensajes de peticiones y respuestas al estilo HTTP para establecer las sesiones.
- Posee también flexibilidad y escalabilidad, diferentes funcionalidades como: proxy, redirección, localización/registro pueden residir en un único servidor o varios distribuidos.
- No es necesario un control centralizado, el funcionamiento de extremo a extremo es posible una vez establecida la sesión. [W16]

Desventajas

- Problemas para resolver direcciones privadas con públicas.
- No atraviesa firewalls ya que tiene problemas con el NAT.

Servidores SIP.- Los Servidores SIP son de tres tipos:

- Proxy Server: Retransmiten las solicitudes que llegan a ellos y deciden a qué otro servidor debe remitirselas, de ser necesario pueden alterar los campos de la solicitud, actúa como cliente y servidor con el propósito de establecer llamadas entre los usuarios, es similar a un Proxy HTTP, existen dos tipos: Statefull Proxy y Stateless Proxy. Statefull Proxy mantienen el estado de las transacciones durante el procesamiento de las peticiones. Permite división de una petición en varias, con la finalidad de la localización en paralelo de la llamada y obtener la mejor respuesta para enviarla al usuario que realizó la llamada, por su parte Stateless Proxy no mantienen el estado de las transacciones durante el procesamiento de las peticiones, únicamente reenvían mensajes. [9]
- Registrar Server: acepta peticiones de registro de los usuarios y guarda la información de estas peticiones para suministrar un servicio de localización y traducción de direcciones en el dominio que controla.
- Redirect Server: es un servidor que genera respuestas de redirección a las peticiones que recibe. Este servidor reencamina las peticiones hacia el próximo servidor.

Este protocolo está basado en una arquitectura de cliente-servidor, las peticiones son generadas por un cliente y enviadas a un servidor que las procesa y devuelve la respuesta al cliente, además el par petición-respuesta recibe el nombre de transacción, proporciona un conjunto de solicitudes y respuestas basadas en códigos, en la Tabla 5.7, se encuentran los métodos de SIP para establecer una llamada. [W3]

Tabla 5. 7 Métodos para el establecimiento de una llamada

METODO	DESCRIPCIÓN
SIP ACK	Confirma el establecimiento de la llamada
SIP BYE	Termina una sesión
SIP CANCEL	Cancela una invitación pendiente

SIP REGISTER	Registra una localización con un servidor Registrar SIP
SIP RE-INVITE	Cambia una sesión actual

PROTOCOLO IAX

Inter Asterisk Exchange protocol.- es uno de los protocolos utilizado por Asterisk, utilizado para manejar conexiones VoIP entre servidores Asterisk, y entre servidores y clientes que también utilizan protocolo IAX.

Las principales características del protocolo IAX son:

- Minimizar el ancho de banda usado en las transmisiones de control y multimedia de VoIP.
- Evitar problemas de NAT (Network Address Translation).
- Soporte para transmitir planes de marcación.
- IAX utiliza un solo puerto (4569) para enviar los datos conjuntamente con la información de señalización, SIP utiliza 1 puerto de señalización (5060) y dos puertos RTP para la transmisión de voz, esto define una clara ventaja para IAX cuando se tienen gran cantidad de llamadas simultáneas. [W17]

Establecimiento de la llamada en IAX tiene tres fases:

- Inicio de sesión.- El terminal A inicia una conexión y manda un mensaje "new", el terminal llamado responde con un "accept" y el terminal llamante le responde con un "Ack"; el terminal llamado da las señales de "ringing" y el llamante contesta con un "ack" para confirmar la recepción del mensaje; el terminal llamado acepta la llamada con un "answer" y el llamante confirma ese mensaje.
- Flujo de datos.- se mandan los frames en ambos sentidos con la información vocal. Los frames M son mini-frames que contienen solo una cabecera de 4 bytes para reducir el uso en el ancho de banda. Los frames F son frames completos que incluyen información de sincronización. Es importante volver a resaltar que en IAX este flujo utiliza el mismo protocolo UDP que usan los mensajes de señalización evitando problemas de NAT.
- Liberación de la llamada o desconexión.- se envía un mensaje de "hangup" y confirmar dicho mensaje. [12]

5.2.2.3. Dispositivos de telefonía IP

TERMINALES IP

Es un dispositivo que permite mantener una comunicación utilizando una red IP, en una red de área local o Internet. Al ser un sistema completamente digital y programable, dispone de un teclado configurable mediante un sistema de administración que puede ser accedido mediante web o mediante telnet. Algunos equipos incluyen cámara de vídeo para poder realizar videoconferencias, se les asigna una dirección IP y se le puede aplicar características como: QoS o VLAN. [9]

ADAPTADOR PARA TELÉFONOS ANALÓGICOS (ATA)

El Analog Telephone Adapter (ATA), tienen un conector FXS para teléfono analógico normal y envían por IP a través del conector LAN, un ATA tiene un conector RJ11 y un RJ45.

SOFTPHONES

Son programas que permiten llamar desde el ordenador utilizando tecnologías IP, se ejecutan en estaciones de trabajo permitiendo establecer llamadas de voz sobre el protocolo IP, este software se lo usa para los casos en los que no se desea colocar teléfonos con el objetivo de reducir los costos en implementación.

CENTRALES IP

Es un equipo diseñado para ofrecer servicios de comunicación a través de las redes de datos, con los componentes adecuados se puede manejar un número ilimitado de anexos en sitio o remotos vía internet, dentro de las funciones de una central telefónica se encuentran:

- Número ilimitado de extensiones
- Múltiples operadores automáticos con menús
- Múltiples casillas de correos de voz
- Integración con teléfonos celulares
- Perifoneo con altavoz
- Teléfonos remotos alrededor del mundo
- Interfaz con el usuario (incluyendo reenvíos, mensajería unificada, grabaciones de los mensajes redirigidos a su correo de voz)
- Rango de Numeración de Extensiones Flexible

- Identificador de llamadas
- DID ingreso directo para marcación interna
- Enrutamiento de llamadas
- Grabación de llamadas
- Grabación en vivo
- Devolución de llamadas
- Correos de voz enviados a sus correos electrónicos
- Notificación por mensajes SMS de sus correos de voz
- Acceso de correo de voz por la Web
- Soporta teléfonos analógicos
- Llamadas en espera
- Llamada monitorizadas
- Integración con el cliente (CRM)
- Servidores vinculados remotos
- Consola de operadora
- Salas de conferencias virtuales
- Números de marcación rápida (Memorias)
- Múltiples Músicas en espera
- Troncales Analógicas y Digitales T1/E1
- Enrutamiento avanzado (IVR)
- Notificación de estatus de llamada
- Aviso de Llamada
- Auto desvío de llamadas
- Mensajería unificada
- Filtrado de llamadas
- Teléfonos virtuales en su PC (Softphones)
- Transferencia de llamadas
- Llamada de conferencia

GATEWAY IP

Ayuda a convertir las llamadas de voz, entre una red IP y la red telefónica pública conmutada a una central digital, tienen interfaces analógicos o digitales a la red telefónica, y disponen de interfaces Ethernet, Frame Relay o ATM hacia la red IP, los puertos FXS Y FXO, es el nombre que se le da a cada puerto que es usado por las líneas telefónicas analógicas.

- FXS.- interfaz de abonado externo, es el puerto que efectivamente envía la línea analógica al abonado, se lo puede comparar con el enchufe de la pared que envía tono de marcado, corriente para la batería y tensión de llamada.
- FXO.- Es la interfaz de central externa, es el puerto que recibe la línea analógica, se lo compara con el enchufe del teléfono, o el enchufe de la central telefónica analógica. [W18]

Estos puertos FXO y FXS son siempre pares, es decir, similares a un enchufe macho/hembra.
En la Fig 5.9, se muestra un caso sencillo sin central IP, el teléfono se conecta directamente al puerto FXS que brinda el proveedor de telefonía.

Fig 5. 9 Uso de los FXS y FXO, sin el uso de una central IP.

En la Fig 5.10, se muestra el caso en el que se incorpora una central IP, debe conectar las líneas que brinda el proveedor de telefonía a la central IP y posterior los teléfonos a la central. Por lo tanto, la central debe tener puertos FXO, para conectarse a los puertos FXS que suministra la empresa telefónica y puertos FXS para conectar los dispositivos de teléfono. [W18]

Fig 5. 10 Uso de los FXS y FXO, con el uso de una central IP.

5.2.2.4. Codecs de voz

Para realizar el dimensionamiento de la red primero debemos elegir el códec de voz a utilizar, la Tabla 8 muestra brevemente los codecs de voz más utilizados y posteriormente se describen algunos de ellos. [W4]

Tabla 5. 8 Información de los CODEC's de voz

Información de códec				Cálculos de ancho de banda					
Velocidad de bits y códec (kbps)	Ejemplo de tamaño del códec (bytes)	Ejemplo de intervalo del códec (ms)	Mean Opinion Score (MOS)	Tamaño de la carga útil de voz (bytes)	Tamaño de la carga útil de voz (ms)	Paquetes por segundo (PPS)	Ancho de banda MP o FRF.12 (kbps)	Ancho de banda c/cRTP MP o FRF.12 (kbps)	Ancho de banda Ethernet (kbps)
G.711 (64 kbps)	80 bytes	10 ms	4,1	160 bytes	20 ms	50	82,8 kbps	67,6 kbps	87,2 kbps
G.729 (8 kbps)	10 bytes	10 ms	3,92	20 bytes	20 ms	50	26,8 kbps	11,6 kbps	31,2 kbps
G.723.1 (6.3 kbps)	24 bytes	30 ms	3,9	24 bytes	30 ms	34	18,9 kbps	8,8 kbps	21,9 kbps
G.723.1 (5.3 kbps)	20 bytes	30 ms	3,8	20 bytes	30 ms	34	17,9 kbps	7,7 kbps	20,8 kbps
G.726 (32 kbps)	20 bytes	5 ms	3,85	80 bytes	20 ms	50	50,8 kbps	35,6 kbps	55,2 kbps
G.726 (24 kbps)	15 bytes	5 ms		60 bytes	20 ms	50	42,8 kbps	27,6 kbps	47,2 kbps
G.728 (16 kbps)	10 bytes	5 ms	3,61	60 bytes	30 ms	34	28,5 kbps	18,4 kbps	31,5 kbps

G.711

Es un estándar de la ITU-T para la compresión de audio empieza a ser usado desde el año 1972, principalmente en telefonía, es un estándar para representar señales de audio con frecuencias de la voz humana, proporciona un flujo de datos de 64 kbit/s, para este estándar existen dos algoritmos principales, la ley-μ (usado en Norte América y Japón) y la ley-A (usado en Europa y el resto del mundo) [12][9]

Características

- Frecuencia de muestreo de 8KHz
- Tasa de bit de 64kbps (8kHz frecuencia de muestreo por 8 bits por muestra)
- Retardo típico del algoritmo 0.125ms

- G.711 Apéndice I define un algoritmo PLC (Packet Loss Concealment) para ayudar a ocultar pérdidas de transmisión en una red de paquetes.
- G.711 Apéndice II define un algoritmo DTX (Discontinuous Transmission), el cual es usado con VAD (Voice Activity Detection) y CNG (Confort Noise Generation) para reducir el ancho de banda durante los periodos de silencio.

G.729

G.729 comprime audio de voz en tramas de 10 milisegundos, se usa frecuentemente en aplicaciones de Voz sobre IP debido a sus bajos requerimientos en ancho de banda, opera a una tasa de bits de 8 kbit/s, pero existen extensiones, las cuales suministran también tasas de 6.4 kbit/s y de 11.8 kbit/s para peor o mejor calidad en la conversación respectivamente. [12][9]

Extensiones

- G.729A, menos complejidad, menor procesamiento, pero la calidad de conversación se empeora marginalmente.
- G.729B, utiliza compresión de silencio, mediante un módulo VAD detecta la actividad de voz y no transmite los silencios. Incluye un módulo DTX el cual decide actualizar los parámetros de ruido de fondo para la ausencia de conversación (entornos ruidosos). Estas tramas que son transmitidas para actualizar los parámetros del ruido de fondo se llaman tramas SID. También hay un generador de ruido de confort (CNG), dado que en un canal de comunicación, si se detiene la transmisión, a causa de ausencia de conversación, entonces el receptor puede suponer que el enlace se ha roto.
- G.729.1, suministra soporte para conversación de banda ancha y codificación de audio, el rango de frecuencia acústica se extiende a 50Hz – 70kHz. Su tasa de bits y la calidad obtenida es ajustable por un simple truncado de la corriente de bits.

G.726

Adaptive Differential Pulse Code Modulation, ADPCM estándar ITU-T, fue pensado para reemplazar a G.721 que cubría ADPCM a 32 kbps y G.723 que cubrió ADPCM también a 24 y 40 kbps, el más usado comúnmente es a 32 kbps, debido a que utiliza la mitad de la tasa del codec G.711, aumentando la capacidad de ancho de banda de red en un 100%. [12][9]

Características:

- Frecuencia de muestreo de 8 KHz
- Tasas de bits disponibles: 16, 24, 32 y 40 kbps.
- Genera una corriente de bits, por lo tanto el tamaño de trama es determinada por la paquetización (típicamente 80 muestras por una trama de 10 ms)
- Retardo típico del algoritmo 0.125ms
- Utiliza el algoritmo de codificación ADPCM

G.723.1

Comprime el audio de voz en tramas de 30 ms, puede operar a dos tasas de bits: 6.3 kbps (con una trama de 24 bytes) usando el algoritmo de codificación MPC-MLQ y a 5.3 kbps (con tramas de 20 bytes) utilizando ACELP como algoritmo de codificación. [9]

Características:

- Frecuencia de muestreo de 8Khz/16 bit (240 muestras por tramas de 30ms)
- Tasas de bits fijas (5.3 kbps con tramas de 20 bytes de 30ms, 6.3 kbps con tramas de 24 bytes de 30ms)
- Retardo del algoritmo 37.5 ms por trama
- Define una trama SID (Silence Insertion Descriptor) de 4 bytes para CNG (Confort Noise Generation)

En un análisis de los beneficios de los Codecs de audio, se ha podido identificar que el Codec G.711 tiene una buena calidad de llamada, sin embargo su consumo de ancho de banda es alto, debido a los servicios que prestará la red para cada Infocentro el uso de este códec de voz no resulta adecuado por su alto requerimiento de ancho de banda. [W4]

El Codec G.723.1 tiene un bajo consumo del ancho de banda, con una calidad de voz regular, debido a que el servicio de VoIP cursará a través de una red VPN, se requiere que la calidad de voz sea buena por lo que este Codec de voz no se recomienda para este propósito.

El Codec de voz G.729 tiene un consumo de ancho de banda relativamente bajo y buena calidad de voz, sin embargo su desventajas de este códec es que no es de uso abierto, se debe pagar una licencia por cada canal para llamada concurrente (llamada simultanea), el costo de cada licencia es de $10, 00 USD, de acuerdo a lo que se indica en la página www.digium.com, teniendo en cuenta que el consumo de ancho de banda por cada servicio debe ser bajo, con una buena calidad de llamada se considera que los beneficios del uso de este códec superan el costo que este representa, por tanto se opta por el uso de este códec de voz para el diseño de esta red.

5.2.2.5. Elección de los terminales IP

Tabla 5. 9 Comparativo de los terminales IP.

CARACTERÍSTICAS DE LOS TERMINALES IP				
	YEALINK-T19P	**Polycom VVX 201**	**Cisco SPA 502G**	**Panasonic KX-HDV130**
APARIENCIA				
CODECS	G.711(A/µ), G.723 G.729AB G.726	G.711 (A-law and µ-law), G.729AB G.722 (HD Voice) iLBC	G.711 (A-law and µ-law) G.726 (16/24/32/40 kbps) G.729 AB G.722	G.711 (A-law and µ-law) G.726 (16/24/32/40 kbps) G.729 AB
PROTOCOLO QUE SOPORTA	SIP v1, IPv6, IPv4, HTTP/HTTPS, QoS: 802.1p, SRTP	SIP Protocol Support FTP/FTPS/TFTP/HTTP/HTTPS DHCP, QoS Support–IEEE 802.1p/Q RTCP and RTP support TCP, UDP, DNS-SRV	MAC address, IPv4, ARP, DHCP ICMP, TCP, UDP RTP, RTCP, DiffServ, ToS	--

			QoS 802.1p/Q	
CONECTIVIDAD	2 Puertos RJ45 10/100 BaseTX	2 Puertos RJ45 10/100 BaseTX	2 Puertos RJ45 10/100 BaseTX	2 Puertos RJ45 10/100 BaseTX
FUNCIONES PRINCIPALES	Llamada en espera Desvío, transferencia, rechazo de llamada Voicemail, Marcaciones rápidas, Ajuste de Volumen, Selección de timbre Multi idioma Agenda: 1000 registros.	Llamada en espera Desvío, transferencia, rechazo de llamada Ajuste de Volumen, Selección de timbre	Navegación en la interfaz usuario por menús, Función de división de líneas, Llamada en espera, música de espera, Transferencia de llamadas	Llamada en espera Desvío, transferencia, rechazo de llamada Ajuste de Volumen, Selección de timbre
ALIMENTACIÓN	PoE (802.3af), AC Power	PoE (802.3af), AC Power	PoE (802.3af), AC Power	PoE (802.3af), AC Power
PRECIO APROXIMADO	$65.95	$ 134.00	$ 143.00	$82.42

De los equipos terminales ya mencionados se decide el uso de los teléfonos IP de la marca Panasonic, debido a que estos cuentan con las características seleccionadas en este estudio como son: Codec de voz G.729, Protocolo SIP, y las funciones básicas de operación; a un precio cómodo. [W5][W6][W7][W8]

5.2.2.6. Elección del servidor VoIP

La solución que se plantea para el servicio de VoIP, se basa en el uso del Software Libre mediante Elastix, desarrollado por la empresa ecuatoriana Palo Santo Solutions, implementa gran parte de su funcionalidad sobre 4 programas de software muy importantes como son Asterisk, Hylafax, Openfire y Postfix; estos brindan las funciones de PBX, Fax, Mensajería Instantánea e Email, respectivamente, Fig. 5.11. La parte de sistema operativo se basa en CentOS, una popular distribución Linux orientada a servidores, la principal ventaja de Elastix es su interfaz Web que le hace mucho más amigable y de fácil administración.[10]

Fig 5. 11 Servicios de Elastix

5.2.2.7. Características y funcionalidades de Elastix

Elastix tiene múltiples características y funcionalidades relacionadas con los servicios que presta: Telefonía IP, Servidor de Correo, Servidor de Fax, Conferencias, Servidor de Mensajería Instantánea, entre otros, a continuación se enumeran algunas de sus principales características dependiendo del servicio que prestan: [10]

TELEFONÍA IP

- Grabación de llamadas
- Correo de Voz
- Codecs soportados: ADPCM, G.711 (A-Law & µ-Law), G.722, G.723.1 (pass through), G.726, G.728, G.729, GSM, iLBC, entre otros.
- IVR Configurable y Flexible
- Soporte para Sintetización de Voz
- Herramienta para la creación de extensiones por lote

- Cancelador de eco integrado
- Interfaz de detección de Hardware
- Servidor DHCP para asignación dinámica de Ips
- Panel de Operador basado en Web
- Parqueo de llamadas
- Reporte de detalle de llamadas (CDR)
- Tarifación con reporte de consumo por destino
- Reportes de uso de canales
- Asterisk en tiempo real
- Centro de Conferencias con Salas Virtuales
- Soporte para protocolos SIP e IAX, entre otros
- Correo de voz-a-Email
- Soporte para Interfaces Análogas como FXS/FXO (PSTN/POTS)
- Soporte para interfaces digitales E1/T1/J1 a través de los protocolos PRI/BRI/R2
- Identificación de llamadas (Caller ID)
- Troncalización
- Soporte para follow-me
- Soporte para grupos de timbrado
- Soporte para paging e intercom
- Soporte para condiciones de tiempo
- Soporte para PINes de seguridad
- Soporte para DISA (Direct Inward System Access)
- Soporte para Callback
- Soporte para interfaces tipo bluetooth a través de teléfonos celulares (chan_mobile)
- Configuración de proveedores de VoIP

FAX

- Servidor Fax basado en HylaFax
- Visor de faxes integrado con PDFs descargables
- Aplicación fax-a-email
- Envío de fax desde interfaz web
- Personalización de faxes-a-email
- Control de acceso para clientes de fax
- Puede ser integrada con Winprint Hylafax

MENSAJERÍA INSTANTANEA

- Servidor de mensajería instantánea basado en OpenFire
- Inicio de llamadas desde cliente de mensajería
- Servidor de mensajería es configurable desde Web
- Soporta grupos de usuarios
- Soporta conexión a otras redes de mensajería como MSN, Yahoo Messenger, GTalk, ICQ
- Reporte de sesiones de usuarios
- Soporte XMPP/Jabber
- Soporte de Plugins
- Soporte LDAP
- Soporta conexiones server-to-server para compartir usuarios

EMAIL

- Servidor de Email con soporte multi dominio
- Administración centralizada vía Web
- Interfaz de configuración de Relay
- Cliente de Email basado en Web
- Administración de Lista de Email
- Soporte para cuotas
- Soporte Antispam
- Basado en Postfix para un alto volumen de correos
- Módulo de SMTP Remoto

5.3. DISEÑO DE LA TOPOLOGÍA DE LA RED VPN, PARA EL INTERCAMBIO DE VOZ, VIDEO Y DATOS ENTRE LOS INFOCENTROS COMUNITARIOS.

VPN (Virtual Private Network) es una extensión de una red local y privada, utiliza como medio de enlace una red pública (Internet), que permite enlazar dos o más redes simulando una única red privada permitiendo así la comunicación entre computadoras como si fuera punto a punto.

Utilizan tecnología de túnel (tunneling) para la transmisión de datos mediante un proceso de encapsulación y en su defecto de encriptación, la implementación de una red VPN es la de reducir notablemente los costos de comunicación.

5.3.1. Ventajas de una VPN

- Seguridad.- los paquetes viajan encriptados a través de un túnel, utilizando las infraestructuras públicas (Internet), estas seguridades hacen que esta información se ilegible para quienes intercepten estos paquetes.
- Bajos costos de implementación.- los costos de implementación de una VPN, tiene que ver más con la capacitación del personal de sistemas para la implementación y mantenimiento de la red privada virtual, además de los costos de contratación de servicios de un ISP, estos dos rubros significan sin embargo una gran oportunidad de ahorro frente a otras tecnologías en donde se tiene que rentar líneas dedicadas, además del ahorro que representa la implementación y configuración de equipos para varios accesos remotos. [14]
- Diseño de la red.- sus topologías de red son de fácil uso y simplicidad.

5.3.2. Elementos de una conexión VPN.

La Tabla 5.11 y la Fig 5.12, menciona brevemente los elementos de una red VPN.

Tabla 5. 10 Elementos de una Red VPN.

ELEMENTO	DETALLE
Servidor VPN	Administra clientes VPN
Cliente VPN	Cliente Remotos
Túnel	Encapsulamiento de los datos
Conexión VPN	Encriptación de datos
Protocolos de Túnel	Administración de túneles
Datos de Túnel	Datos que se transmiten
Red de Tránsito	Red pública de enlace

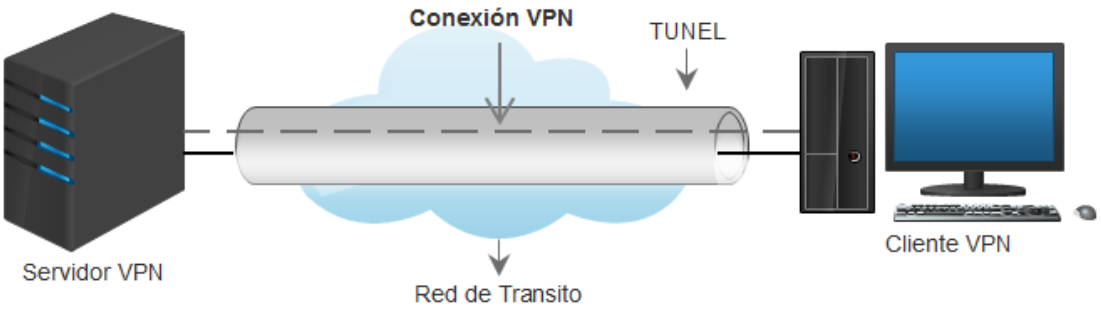


Fig 5. 12 Elementos de una red VPN

- Servidor VPN.- Un equipo que acepta conexiones VPN de clientes VPN, encargado de administrar todos los clientes VPN y proporcionar la seguridad de la red.
- Cliente VPN.- Un equipo que inicia una conexión VPN a un servidor VPN. Un cliente VPN puede ser un equipo individual o un enrutador.
- Túnel.- La parte de la conexión en la que se encapsulan los datos.
- Conexión VPN.- La parte de la conexión en la que se encriptan los datos.
- Protocolos de túnel.- Se utilizan para administrar los túneles y encapsular los datos privados.
- Red de tránsito.- Red pública o compartida que permite el tránsito de los datos encapsulados, pueden ser: Internet o una intranet privada.

5.3.3. Requisitos de una red privada virtual

Para garantizar la operatividad de VPN es necesario cumplir con ciertos requisitos esenciales:

- Disponibilidad.- se aplica tanto al tiempo de actualización como al tiempo de acceso.
- Control.- debe ser implementado por el supervisor o administrador de la Red Privada Virtual, a fin de garantizar el control sobre la misma.
- Compatibilidad.- una VPN se basa en el protocolo IP, por tanto es necesario que la arquitectura interna del protocolo de red de la empresa en donde se va a aplicar VPN, sea compatible con el protocolo IP.
- Seguridad.- una VPN poseen de cifrado y autenticación de usuarios para garantizar la seguridad de la red.

- Interoperabilidad.- es importante para la transparencia en la conexión entre las partes involucradas.
- Confiabilidad.- en la VPN de Acceso Remoto en las que se sujeta a la confiabilidad que se tiene por parte del ISP, si el servicio del ISP se interrumpe, la conexión también lo hará, no se podrá hacer nada hasta que el ISP nuevamente brinde su servicio a los clientes.
- La autenticación de datos.- afirma que los datos han sido entregados a su destinatario totalmente sin alteraciones de ninguna manera.
- La autenticación de usuarios.- es el proceso en el que se controla que solos los usuarios admitidos tengan acceso a la red.
- Sobrecarga de tráfico.- un paquete enviado en una VPN es encriptado y encapsulado, este proceso aumenta de manera significativa la sobrecarga de tráfico en la red.
- Sin repudio.- Consiste en el proceso de identificar correctamente al emisor, con la finalidad de tener claro desde donde proviene la solicitud.

5.3.4. Tipos de redes VPN de acuerdo a su aplicación

Las redes VPN son clasificadas de acuerdo a su aplicación, existen algunas variantes, sin embargo, son 4 tipos los claramente identificados: [16]

5.3.4.1. VPN de sitio a sitio

Son utilizadas para conectar sitios geográficamente separados de una corporación o empresa, a través de internet, los costos de la comunicación se reducen debido a que el cliente sólo paga por su conexión a Internet. Las oficinas remotas se conectan a través de túneles creados sobre Internet, las VPN de sitio a sitio pueden subdividirse a su vez en VPN intranet y VPN extranet.

- VPN de Intranet.- crea una conexión entre las oficinas centrales y las oficinas remotas que se encuentran en el exterior, un enrutador realiza una conexión VPN de sitio a sitio que conecta dos partes de una red privada. El servidor VPN proporciona una conexión enrutada a la red a la que está conectado el servidor VPN, la Fig 5.13 muestra una red VPN intranet. [W19]

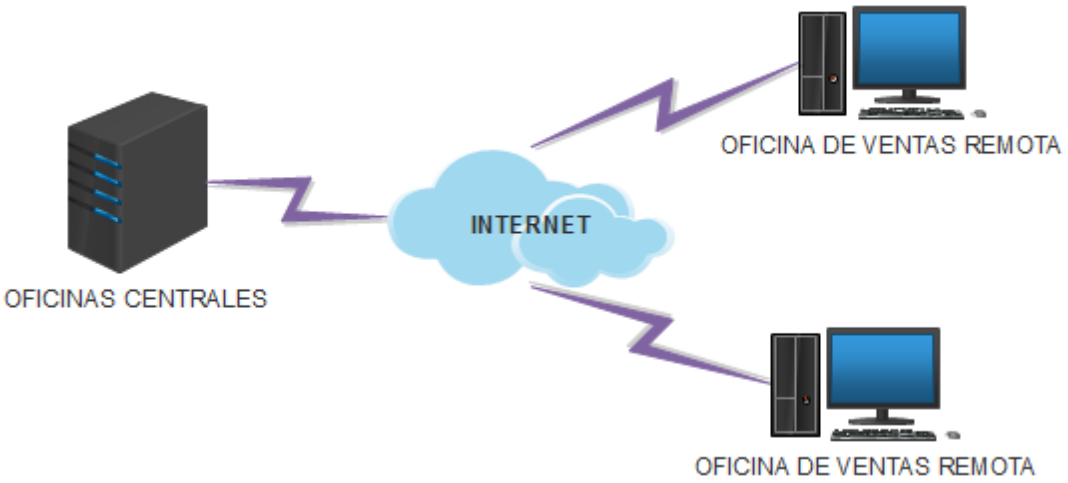


Fig 5. 13 Esquema de una red VPN Intranet.

- VPN de Extranet.- se crea entre la empresa y sus socios comerciales, por ejemplo: clientes o proveedores, mediante el protocolo HTTP (navegadores de Web), para implementar una VPN extranet se debe realizar un acuerdo entre miembros de las distintas empresas u organizaciones entre las que se desea tener conexión. Las empresas disfrutan de las mismas normas que las de una red privada, una de las desventajas de este tipo de red es que la seguridad es vulnerable en comparación con una intranet, por lo que una VPN extranet debe ser diseñada con muchas pólizas de control de acceso y acuerdos de seguridad entre los miembros de la extranet, la Fig 5.14 muestra una red VPN extranet.

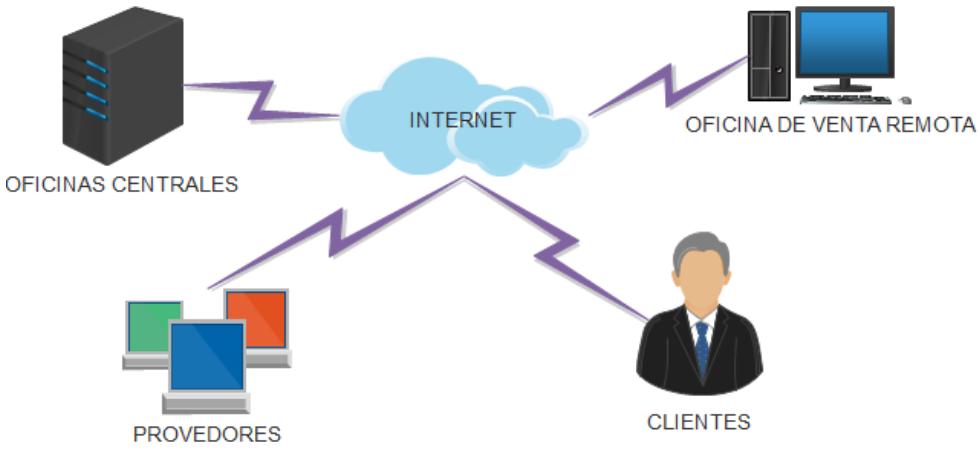


Fig 5. 14 Esquema de una red VPN Extranet.

5.3.4.2. *VPN de acceso remoto*

Se crea entre las oficinas centrales y los usuarios móviles a través de un ISP, el usuario móvil levanta una conexión telefónica con un ISP y crea un túnel de conexión hacia las oficinas centrales.

El cliente de acceso remoto inicia una conexión VPN a través de Internet con el servidor VPN de la compañía. Una vez que se ha establecido el enlace, el usuario puede acceder a los recursos de la intranet privada de la empresa, la Fig 5.15 muestra una red VPN de acceso remoto.

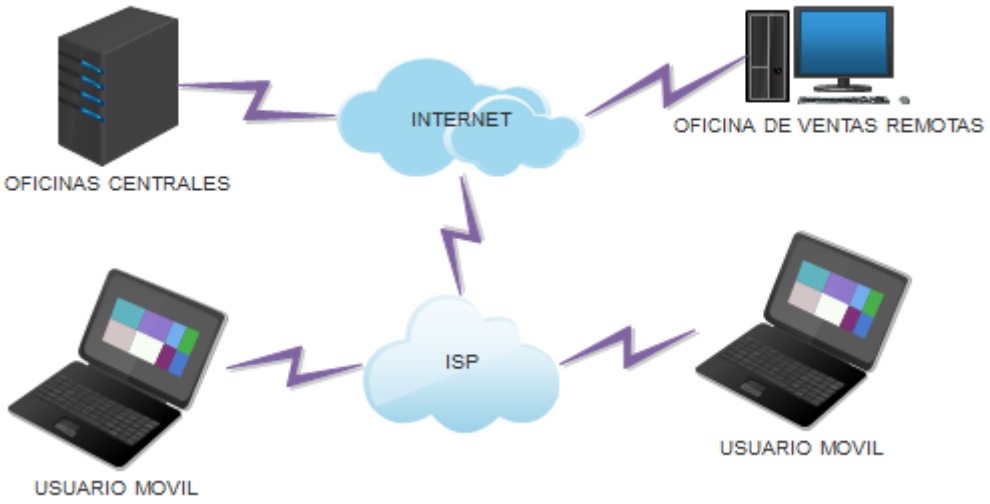


Fig 5. 15 Esquema de una red VPN de Acceso Remoto

5.3.4.3. *VPN interna*

Este tipo de implementación es la menos utilizada, se crea en una LAN, siempre que se considere necesario transferir información con mucha privacidad entre departamentos de una empresa, la Fig 5.16 muestra una red VPN interna.

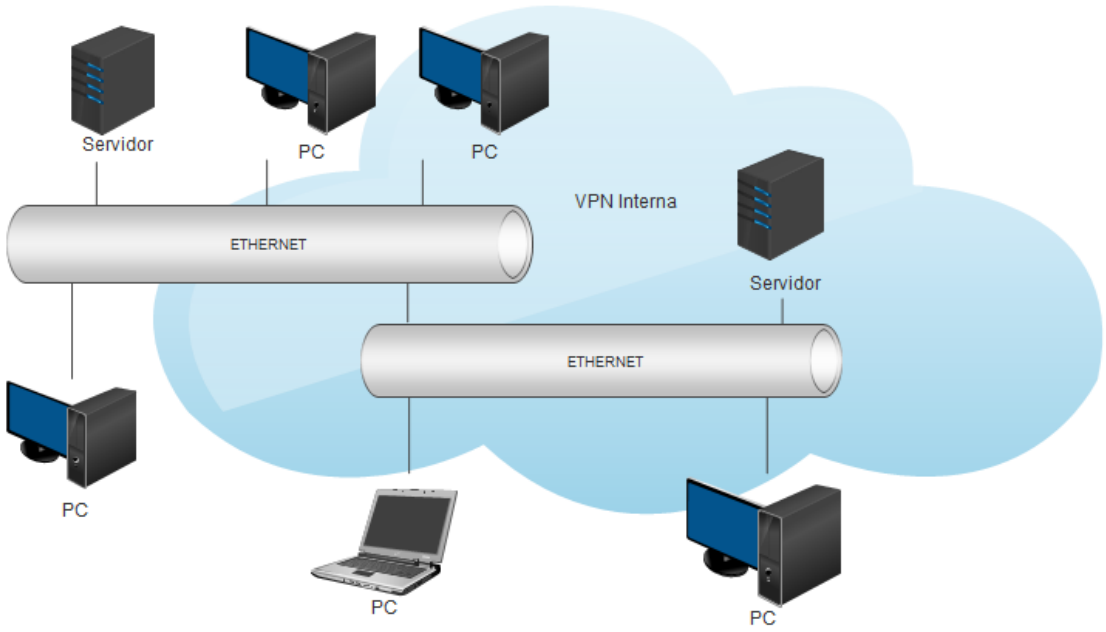


Fig 5. 16 Esquema de una red VPN interna.

5.3.5. Tipos de redes VPN de acuerdo a su modo de implementación.

Los tipos de VPN, de acuerdo a su modo de implementación son: [16]

5.3.5.1. VPN de firewall

Un firewall (llamado también cortafuegos o servidor de seguridad) es un método de seguridad que establece normas de control de acceso entre dos o más redes, un filtro que controla las comunicaciones que pasan de una red a la otra y en función de lo que sean permiten o deniega su paso, el firewall reconoce si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no. Este tipo de VPN es común empresas como Cisco Systems, ofrecen en sus dispositivos firewall soporte para VPN.

Ventajas:

- Arquitectura de red simplificada, al establecer un único punto de control de seguridad.
- Fácil administración

Desventajas:

- La configuración del equipo firewall se convierte en más compleja

- Se exige mayor rendimiento del firewall, ya que este lleva también la configuración de VPN.
- No se tiene hardware especializado de encriptación.

5.3.5.2. VPN de router

Empresas como Cisco, Nortel y 3Com ofrecen servicios VPN integrados dentro de un router o un dispositivo llamado concentrador VPN, por lo que se trata de la solución VPN más rápida, pueden ser configuradas para utilizar certificados, servicios de autenticación externos o claves de seguridad. [W19]

Ventajas:

- Ofrecen un gran rendimiento, porque no malgastan ciclos de procesador haciendo funcionar un Sistema Operativo.
- Es hardware dedicado.
- Capacidad de asegurar el flujo de paquetes entre dos redes, a través de
- una red pública como Internet.
- Capacidad de autentificar y autorizar a usuarios el acceso sobre redes privadas.

5.3.5.3. VPN de sistema operativo

Sistemas operativos como Windows o Linux ofrecen servicios de VPN ya integrados, estos sistemas son ideales para las situaciones donde los dos puntos de conexión de la VPN no están controlados por la misma organización, o cuando los diferentes cortafuegos o routers no son implementados por la misma organización.

Ventajas:

- Es una solución muy económica.- en un mismo sistema operativo se pueden contar con una gran diversidad de servicios y mejora los métodos de autenticación y la seguridad del sistema operativo.

Desventajas:

- Es vulnerable a los problemas de seguridad del propio sistema operativo.
- Estas VPN se utilizan más para el acceso remoto.

5.3.5.4. VPN de aplicación

Es un programa que añade posibilidades VPN a un sistema operativo. Sin embargo, este programa no queda integrado con el sistema operativo.

Ventajas:

- La aplicación añade seguridad extra a la que podría ofrecer una VPN integrada al sistema operativo.

Desventajas:

- No soportan una gran cantidad de usuarios.
- Son mucho más lentas que una VPN basada en hardware.
- Son vulnerables a las fallas de seguridad del sistema operativo que contiene a la aplicación.

5.3.5.5. VPN de proveedor de servicios

Es proporcionada por un proveedor de servicios. El proveedor de servicios es la empresa propietaria de la infraestructura tales como equipos y líneas de transmisión que ofrece líneas dedicadas virtuales a sus clientes. El cliente se conecta a la red del proveedor de servicios a través de un dispositivo de equipo terminal del cliente como puede ser un router, este se conecta a través de medios de transmisión al equipo del proveedor de servicios, que puede ser X.25, Frame Relay, un conmutador ATM o un router IP. La línea virtual que se le proporciona al cliente mediante el proveedor de servicios se le llama circuito virtual (VC). El proveedor de servicios puede cargar o una tarifa plana para el servicio VPN, que habitualmente depende del ancho de banda disponible para el cliente, o una tarifa basada en el uso, que puede depender del volumen de datos intercambiados o de la duración del intercambio de datos.

5.3.6. Topologías de VPN

La topología de una red VPN debe elegirse dependiendo del requerimiento de la red, podemos encontrar las siguientes topologías:

5.3.6.1. Topologías para VPN de sitio a sitio

TOPOLOGÍA RADIAL.- las sucursales remotas se conectan a un sitio central, la mayor parte del intercambio de datos se da con las oficinas centrales de la compañía, los datos intercambiados entre las sucursales siempre viajan a través del sitio central, la Fig. 5.17 muestra esta topología.

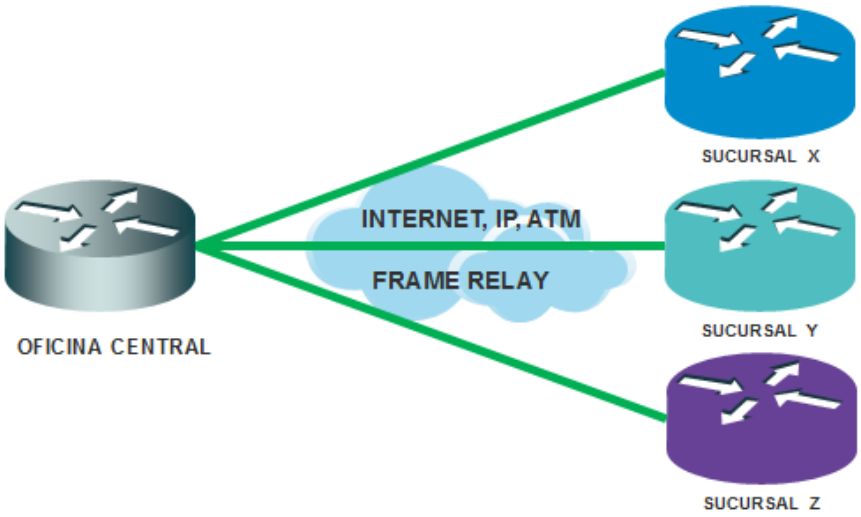


Fig 5. 17 Topología de red VPN en tipo radial.

TOPOLOGÍA DE MALLA COMPLETA O PARCIAL.- es implementada en corporaciones que no tienen una estructura demasiado jerárquica. Aquí, las diversas LAN de la compañía pueden realizar un intercambio constante de datos entre ellas, una empresa puede utilizar una topología de malla completa si todas las LAN se comunican entre sí o una topología de malla parcial, si sólo algunas LAN mantienen intercambio de datos, las Figuras 5.18 y 5.19 muestra un ejemplo de esta topología.

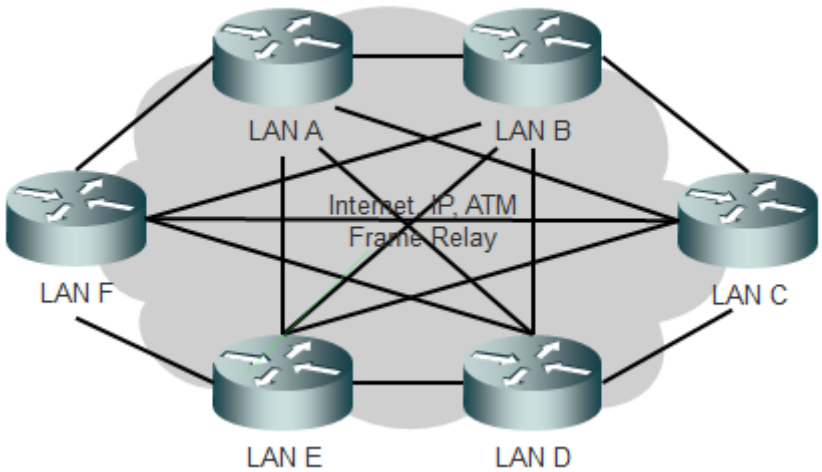


Fig 5. 18 Topología de red VPN tipo malla completa

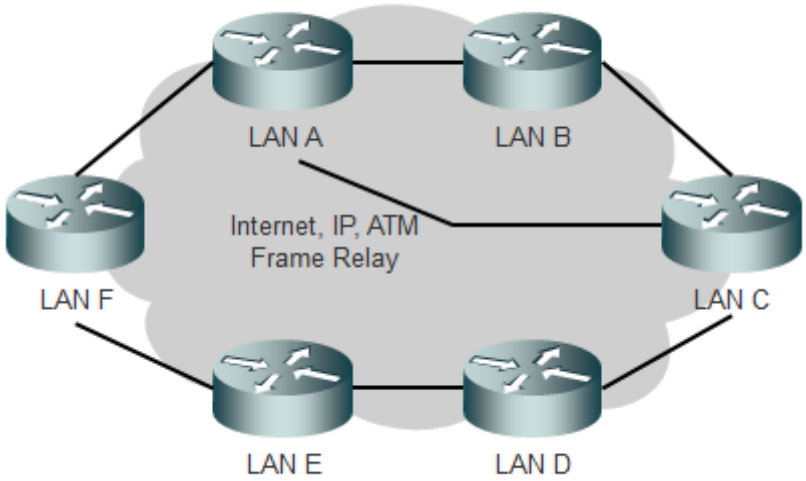


Fig 5. 19 Topología de red VPN tipo malla parcial

5.3.6.2. Topología para VPN de acceso remoto

TOPOLOGÍA DE ACCESO REMOTO.- esta topología consiste en un enlace punto a punto entre el usuario remoto y la oficina central utilizando tramas tunneling PPP intercambiadas entre el usuario remoto y el servidor VPN. El usuario y el servidor establecen conectividad usando un protocolo de capa 3, siendo el más común IP, sobre el enlace PPP entunelado e intercambian paquetes de datos sobre él, su esquema es similar al de tipo radial.

5.3.7. Protocolos de entunelamiento

Haciendo referencia al modelo OSI, se puede crear una VPN usando tecnologías de Tunneling de capa 2 y capa 3, un túnel es similar a levantar una sesión de comunicación; los dos nodos finales del túnel deben estar de acuerdo al túnel y deben negociar las variables de la configuración, asignación de dirección, los parámetros de encriptación o de compresión. En la mayoría de los casos, los datos que se transfieren a través del túnel se envían utilizando protocolos basados en datagramas.

Tunneling es una técnica que usa una infraestructura entre redes para transferir datos de una red a otra, es decir el túnel es un camino lógico por medio del cual los paquetes son encapsulados para que viajen por la red intermedia, para esto el protocolo de tunneling agrega una cabecera adicional que proporciona información de routing, para que los paquetes puedan atravesar la red

intermedia, una vez que las tramas son encapsuladas estas se enrutan a través de un túnel que tiene como puntos finales los dos puntos entre la red intermedia. Cuando un trama encapsulada llega a su destino en la red intermedia, se des encapsula y se envía a su destino final dentro de la red. Las tecnologías más conocidas de Tunneling son: [13]

- IPSec (Internet Protocol Security Tunnel Mode).
- PPTP (Point-to-Point Tunneling Protocol).
- L2TP (Layer 2 Tunneling Protocol).

Estos niveles corresponden al modelo de referencia (OSI). PPTP y L2TP son protocolos de túnel de nivel 2; ambos encapsulan la carga útil en una trama del protocolo punto a punto (PPP) que se enviará a través de la red. Los protocolos de nivel 3 corresponden al nivel de red y utilizan paquetes IP sobre IP y el modo de túnel de seguridad IP (IPSec); estos protocolos encapsulan los paquetes IP en un encabezado adicional IP antes de enviarlos a través de una red IP.

5.3.7.1. Protocolo PPTP

El Protocolo de Túnel Punto a Punto (PPTP, Point-to-Point Tunneling Protocol) es un protocolo de red creado por Microsoft, Ascend Communications y US Robotics, PPTP es una extensión de PPP y opera a nivel de enlace del modelo de referencia OSI, el cual es utilizado tradicionalmente para las conexiones dial-up, permite la realización de transferencias seguras desde clientes remotos a servidores emplazados en redes privadas, empleando para ello tanto líneas telefónicas conmutadas como Internet. [W20]

PPTP encapsula los paquetes PPP en datagramas IP, una vez que los datagramas llegan al servidor PPTP, son desensamblados con el fin de obtener el paquete PPP y descifrados de acuerdo al protocolo de red transmitido.

Una desventaja que tiene PPTP es que no posee un único estándar para la encriptación y la autenticación, ya que se ocupa únicamente de crear un túnel, por lo que le hace un protocolo VPN menos seguro, PPTP requiere de protocolos adicionales para poder autenticar usuarios y encriptar la información.[W20]

El protocolo de túnel de punto a punto (PPTP) utiliza una conexión de TCP (puerto 1723) para el mantenimiento del túnel y las tramas de PPP encapsuladas, las cuales a su vez son encapsuladas en paquetes de encapsulamiento de enrutamiento genérico (GRE) destinadas a los datos en el túnel, la Fig 5.20, muestra la forma en que se ensambla el paquete de PPTP antes de la

transmisión, El diseño de la trama final muestra la encapsulación para un cliente de marcación (controlador de dispositivo PPP).

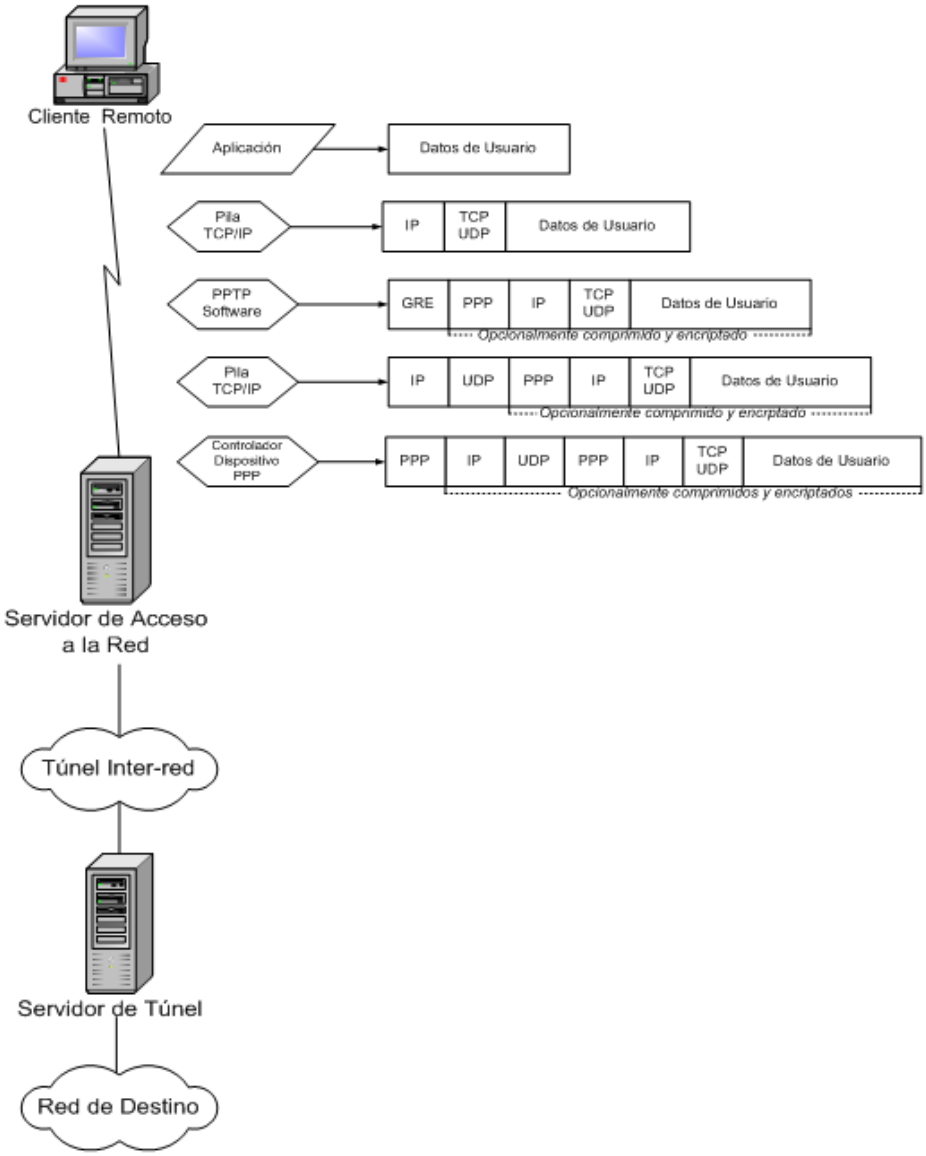


Fig 5. 20 Construcción de un paquete PPTP

5.3.7.2. Protocolo L2TP

L2TP, Layer 2 Tunneling Protocol.- es un protocolo estándar diseñado para transmitir datos y conectar de forma segura redes a través de Internet. L2TP es un protocolo estándar aprobado por el IETF (Internet Engineering Task Force), en oposición al protocolo propietario de Microsoft PPTP, L2TP es una extensión del Protocolo Túnel Punto a Punto usado por los ISP para permitir la operación de VPN sobre Internet. L2TP encapsula las tramas PPP que van a enviarse a través de redes IP, X.25, Frame Relay, o ATM. [13]

Cuando está configurado para utilizar IP como su transporte, L2TP se puede utilizar como protocolo de túnel VPN en Internet. L2TP utiliza UDP para mantener el túnel y para enviar tramas PPP encapsuladas en L2TP como datos del túnel; cuando los túneles L2TP aparecen como paquetes IP, pueden hacer uso de IPSec, en una configuración denominada L2TP/IPSec, lo cual proporciona gran seguridad cuando se transportan datos en redes públicas IP.

L2TP se diseñó específicamente para conexiones de acceso remoto, así como para conexiones sitio a sitio. L2TP requiere del uso de certificados digitales para la autenticación. L2TP es soportado por diferentes sistemas operativos así como routers y firewalls, L2TP usa el puerto UDP 1701. El ensamblado de un paquete L2TP al momento de su transmisión se muestra en la Fig 5.21.

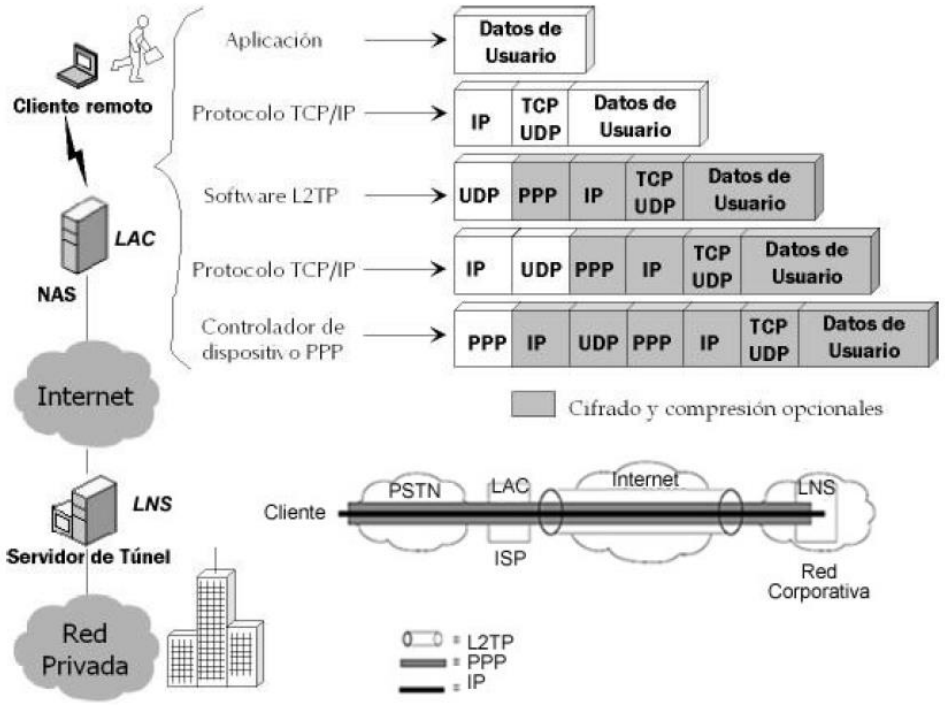


Fig 5. 21 Construcción de un paquete L2TP

Para asegurar L2TP se requiere que el transporte proporcione servicios de encriptación, seguridad y autenticación para todo el tráfico L2TP, este transporte seguro opera sobre el paquete L2TP completo y funciona independientemente de PPP y del protocolo que este siendo transportando por PPP. L2TP sólo se preocupa de la confidencialidad, autenticidad e integridad de los paquetes L2TP entre los extremos del túnel. [W21]

5.3.7.3. Protocolo IPSec

La Seguridad del Protocolo de Internet (IPSec, Internet Protocol Security), se basa en los estándares desarrollados por el grupo de trabajo de IPSec del IETF, se encuentra documentado en diversos RFC de los cuales el principal es el RFC 2401.

IPsec es un conjunto de estándares abiertos cuyo objetivo es conseguir que las comunicaciones sean privadas utilizando las redes IP, esto se lograría mediante el uso de criptográfica que proporciona una sólida protección extremo a extremo, debido a que los únicos equipos que conocen que existe protección con IPSec son el remitente y el receptor de la comunicación, en otras palabras IPSec protege el contenido de los paquetes IP contra ataques de red mediante el filtrado de paquetes. [15]

Cada equipo se encarga de la seguridad en su extremo y asume que el medio de comunicación no es seguro, IPsec puede implementarse en los siguientes casos:

- Red de área local (LAN): cliente-servidor y entre homólogos
- Red de área extensa (WAN): entre routers y entre puertas de enlace
- Acceso remoto: clientes de acceso telefónico y acceso a Internet desde redes privadas

IPSec utiliza dos protocolos que proporcionan seguridad en el tráfico, los cuales son:

- Cabecera de autenticación (AH, Authentication Header).- AH proporciona integridad en la conexión, autenticación de los datos de origen y un servicio opcional contra paquetes repetidos. La cabecera de autenticación (AH, Authentication Header) puede detectar paquetes alterados y puede autenticar la identidad del emisor basándose en el usuario final o en la dirección IP fuente.
- Carga de Seguridad de Encapsulamiento (ESP, Encapsulating Security Protocol).- provee confidencialidad de los datos utilizando técnicas de encriptación, puede proporcionar también autenticación, integridad y protección contra paquetes repetidos. Las primeras versiones de ESP se enfocaron principalmente en la confidencialidad; sin embargo, el estándar final también incluye una gran funcionalidad como la que proporciona AH. Los estándares ESP soportan principalmente dos métodos de cifrado DES y 3DES.

Cada protocolo soporta dos modos de uso: modo transporte y modo túnel; en el modo transporte los AH y ESP proveen protección a los protocolos de capas superiores, en el modo túnel AH y ESP son aplicados para entunelar paquetes IP, también se utiliza un conjunto protocolos necesarios para la gestión de llaves criptográficas: [15]

La Asociación de Seguridad (SA), utilizada para realizar autenticación, se definen todos los servicios de seguridad que deben ser aplicados al tráfico de red, pueden ser creadas automáticamente o manualmente, empleando para ello el protocolo ISAKMP/Oakley e IKE.

ISAKMP (ISAKMP, Internet Security Association and Key Management Protocol), es un sistema de intercambio de claves y autenticación que es independiente de cualquier tecnología de claves específica.

IKE es un diseño específico dentro de un sistema más complejo conocido como Protocolo de Administración de Claves y Asociación de Seguridad de Internet, IKE trabaja con otro protocolo llamado Oakley, para el intercambio de claves seguras dentro del modelo ISAKMP. [15]

5.3.8. Diseño de la red VPN

Para el diseño de la red VPN se considera el escenario el siguiente escenario:

- Tipo de VPN: Sitio a Sitio, en modo intranet, ya que la oficina matriz (MINTEL) desea tener comunicación con sus sucursales (Infocentros).
- Modo de implementación: VPN Router a Router, cada Infocentro cuenta con un router CISCO modelo C881-K9, que permite la configuración de redes VPN y admite los protocolos IP SEC, para la oficina matriz se puede hacer la adquisición de un router CISCO RV082 que permite hasta 100 túneles de IP sec sitio a sitio, en las Tablas 5.11 y 5.12, se muestra las características de las de los routers seleccionados. [W9] [W10]

Tabla 5. 11 Especificaciones Técnicas ROUTER CISCO RV082

CISCO RV082	
ESPECIFICACIONES TÉCNICAS	
	
WAN dual	Configurable para copia de seguridad Smartlink o equilibrio de

	carga
Estándares	802.3, 802.3u, IPv4 (RFC 791).
Protocolos de red	DHCP, IP estática, Protocolo punto a punto a través de Ethernet (PPPoE), Protocolo de tunelación punto a punto (PPTP)
Protocolos de routing	Estático, RIP v1 y v2
Traducción de direcciones de red (NAT)	Traducción de direcciones de puerto (PAT), Traducción de direcciones de red y puerto (NAPT), NAT traversal, NAT uno a uno
Firewall	SPI, denegación de servicio (DoS), IP Spoofing (Suplantación de IP), alerta de correo electrónico para los ataques de hackers
Bloqueo	Java, cookies, ActiveX, proxy HTTP
Filtrado de contenido	Bloqueo de URL estática o bloqueo mediante palabras clave
Gestión protegida	HTTPS, nombre de usuario/contraseña, complejidad de contraseña
VPN	
IPsec	100 túneles de IPsec sitio a sitio para la conectividad de sucursal
QuickVPN	50 túneles de QuickVPN para el acceso de clientes remotos
PPTP	5 túneles de PPTP para el acceso de clientes remotos
Cifrado	Estándar de cifrado de datos (DES), Triple estándar de cifrado de datos (3DES) y Estándar de cifrado avanzado (AES) AES-128, AES-192, AES-256
Autenticación	Autenticación MD5/SHA1
NAT traversal de IPsec	Compatible para túneles de puerta de enlace a puerta de enlace y de cliente a puerta de enlace
Transferencia de VPN	PPTP, L2TP, IPsec
VPN avanzada	Detección de puntos inactivos (DPD), IKE, DNS dividido, copia de seguridad de VPN
Calidad de servicio (QoS)	
Tipos de priorización	Prioridad basada en aplicaciones en el puerto WAN
QoS basada en servicios	Compatibilidad con control de velocidad o prioridad
Control de velocidad	El ancho de banda de flujo ascendente/descendente se puede

	configurar por servicio
Prioridad	Cada servicio puede asignarse a uno de los 3 niveles de prioridad
Rendimiento	
Rendimiento de NAT	200 Mbps
Rendimiento de VPN de IPsec	97 Mbps
Configuración	
Interfaz de usuario Web	Administrador de dispositivos sencillo basado en navegador (HTTP/HTTPS)
Protocolos de gestión	Navegador web, Protocolo simple de administración de red (SNMP) v1 y v2c, Bonjour
Registro de eventos	Syslog, alertas de correo electrónico, monitor del estado del túnel de VPN

Tabla 5. 12 Especificaciones técnicas ROUTER CISCO C881 – K9.

CISCO C881 –K9	
ESPECIFICACIONES TÉCNICAS	
	
IP and IP services features	RIPv1 and RIPv2, Generic routing encapsulation (GRE), Standard 802.1d Spanning Tree Protocol, Layer 2 Tunneling Protocol (L2TP) Network Address Translation (NAT), Dynamic Host Configuration Protocol (DHCP) server,

CISCO C881 –K9	
ESPECIFICACIONES TÉCNICAS	
	
	Access control lists (ACLs)
Security features	SSL VPN for secure remote access Hardware-accelerated DES, 3DES, AES 128, AES 192, and AES 256 20 IPsec tunnels Cisco Easy VPN Client and Server NAT transparency
QoS features	Low-Latency Queuing (LLQ) Weighted Fair Queuing (WFQ) Class-Based WFQ (CBWFQ) Class-Based Traffic Shaping (CBTS) (on Fast Ethernet WAN ports and DSL ports in Packet Transport Mode [PTM] only) Class-Based Traffic Policing (CBTP) Policy-Based Routing (PBR) Class-Based QoS MIB Class of service (CoS)-to-differentiated services code point (DSCP) mapping

La Fig 5.22, muestra el diseño propuesto para la red VPN, con las consideraciones antes mencionadas, la Fig. 5.23 muestra el diseño final de la red VPN con la integración de servicios de VoIP y video vigilancia IP.

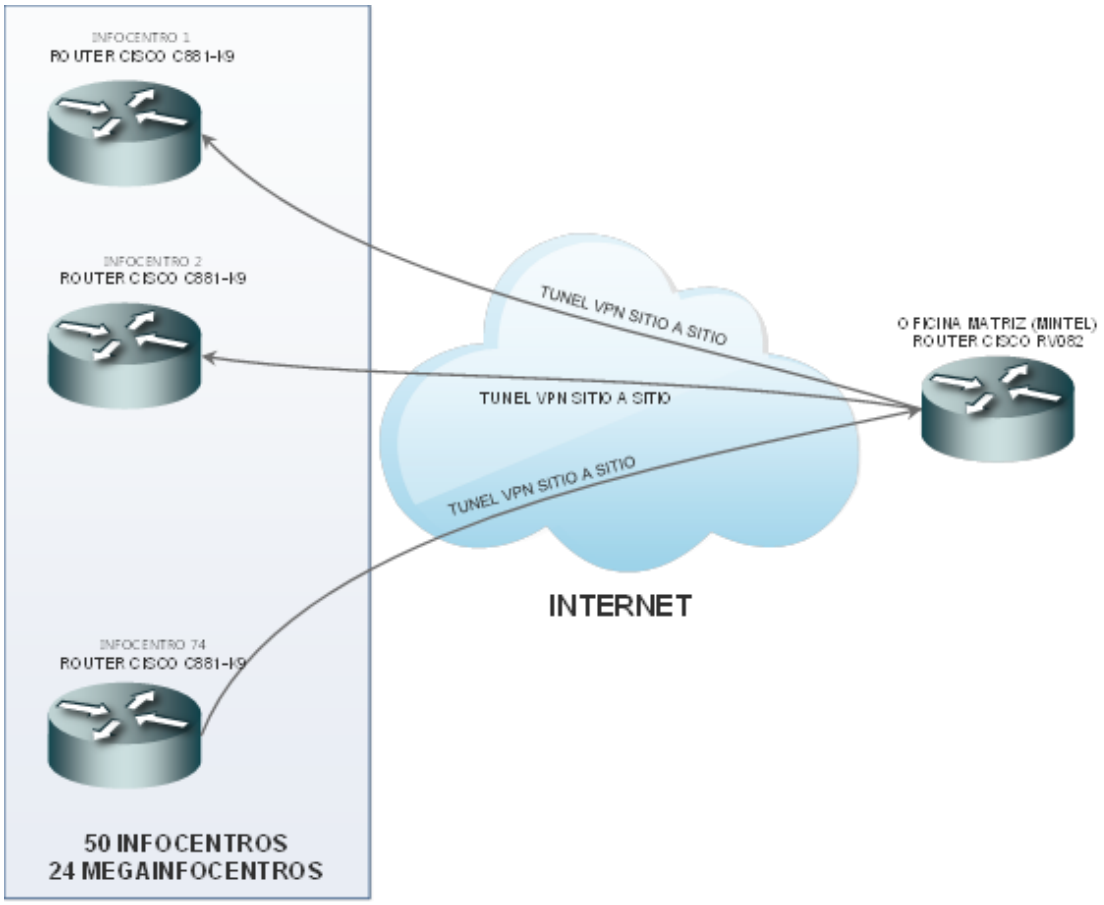
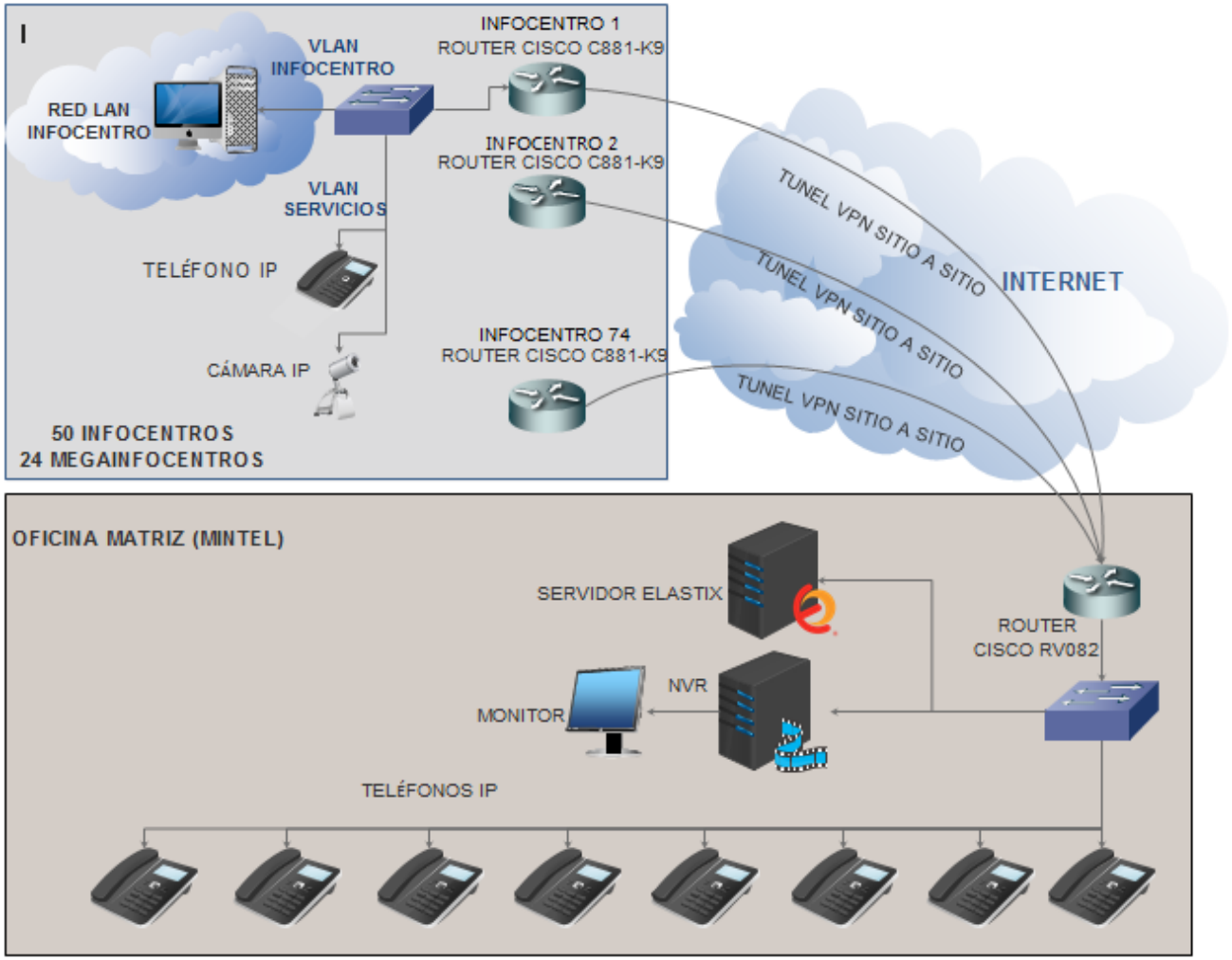


Fig 5. 22 Diseño de La Red VPN.



5.3.9. Diseño de red con la integración de servicios.

5.4. DIMENSIONAMIENTO DEL ANCHO DE BANDA REQUERIDO PARA LA INTEGRACIÓN DE ESTOS SERVICIOS.

5.4.1. Dimensionamiento de tráfico para video

Para el dimensionamiento de tráfico para video se utiliza la ecuación1:

$$C_{video} = \left[\frac{width * heighth * color * color\ bit\ depth * I_{ps}}{factor\ de\ compresion}\right] bps$$

Ecuación 1

De donde:

- C_{video} : Capacidad de video
- $width * heighth$: tamaño de la imagen (pixeles)
- $color\ bit\ depth$: profundidad del color utilizado para las imágenes, 8 bits para codificar cada uno de los tres colores RGB.
- I_{ps} : número de imágenes por segundo
- $factor\ de\ compresion$: factor de compresión de imágenes por video

Para el cálculo del tráfico de video se han tomado en cuenta los siguientes datos con las especificaciones técnicas de la cámara seleccionada.

- $width * heighth$ = 704 * 480 (resolución 4CIF NTSC, muy utilizada para cámaras IP ya que permite ver adecuadamente el video y no genera demasiado tráfico).
- $color\ bit\ depth$ = 8 bits * 3colores = 24 bits
- I_{ps} : 5 Ips
- $factor\ de\ compresion$: se utilizará el estándar de compresión MPEG-4, soporta factores de compresión 70:1 para imágenes en movimiento y 200:1 para imágenes estáticas, al no capturar imágenes en movimiento la totalidad del tiempo, se ha elegido un promedio de factor de compresión de 140.

Sustituyendo en la ecuación 1, quedaría:

$$C_{video\ (bps)} = \left[\frac{704 * 480 * (3 * 8) * 5}{140}\right] bps$$

$$C_{video\ (bps)} = [289645{,}7157]\ bps$$

$$C_{video\ (bps)} = [289{,}65]\ Kbps$$

La capacidad requerida es de 289,65 Kbps por cada cámara, a este valor se lo multiplicará por el total de cámaras que serán instaladas, si consideramos que cada infocentro dispone de un enlace de internet por fibra óptica y que debe tener al menos una cámara de video, el resultado sería el siguiente:

- Número total de Infocentros: 50 Infocentros
- Número total de Megainfocentros: 24 Infocentros

$$C_{(total)} = C_{video} * \#_{Infocentros}$$
$$C_{(total)} = 289{,}65_{\ Kbps} * 74_{\ Infocentros}$$
$$C_{(total)} = 21434{,}1_{\ Kbps}$$
$$C_{(total)} = 21{,}4_{Mbps}$$

Se obtendrá un total de tráfico generado por el video 21,4 Mbps cursando por el enlace de internet que posee la oficina matriz del MINTEL, ya que será el lugar en donde se instale el equipo NVR, para el almacenamiento del video.

El total de tráfico generado por el video que cursará por el enlace de internet en cada Infocentro o Megainfocentro es de 289,65 Kbps, que es el equivalente al ancho de banda que consume una cámara IP.

Una vez que se ha calculado la capacidad de tráfico requerida, se realiza el dimensionado del almacenamiento.

$$289650\frac{bits}{segundo} * \frac{1_{Byte}}{8_{bits}} * \frac{3600_{seg}}{1_{hora}} = 130342500_{Bytes/h}$$

$$130342500\ \frac{Bytes}{h} * \frac{1}{1000} * \frac{1}{1000} = 130{,}34_{\ MB/h} = 0{,}13_{GB/h}$$

Se necesitan 0,13 GB de capacidad de almacenamiento por cada hora de grabación para una cámara.

Debido a la gran capacidad de almacenameinto que se requiere para capturar el video de todos los Infocentros se recomienda que las cámaras IP's sean programadas para que realicen la captura de video al detectar movimiento al interior del Infocentro, lo que supondría se realice en el horario de atención del mismo.

Los Infocentros comunitarios ofrecen su atención al público 8 horas diarias, en un horario casi generalizado de 08:00 – 12:00 y 14:00 – 18:00, durante 5 días de la semana, de este modo tenemos 8 horas de grabación por día, en los 20 días laborables del mes.

$$0{,}13\frac{GB}{h} * \frac{8\,h}{día} * \frac{20\,días}{mes} = 20{,}8\,\frac{GB}{mes}$$

Este cálculo se lo realiza para condiciones normales de funcionamiento del Infocentro, sin embargo, para la elección del equipo grabador de video, se adicionará un 25 % de carga de contenido a fin de cubrir los eventos en los que las cámaras puedan capturar el video fuera de los horarios establecidos debido a la activación de alarmas.

$$20{,}8_{GB} + 25\% = 26_{GB/mes}$$

Debido al número de canales que se requiere que un NVR controle, la instalación de un solo NVR no resultaría util, es por eso que se considera la incorporación de dos equipos de la misma caracteristicas, el equipo seleccionado es un HIKVISION IP DS-9664NI-ST, cuyas caracteristicas se muestran en la Tabla 5.13. [W11]

Tabla 5. 13 Características Técnicas del equipo NVR

GRABADOR NVR IP HIKVISION IP DS-9664NI-ST		
CARACTERÍSTICAS TÉCNICAS		
Cámaras soportadas:	Hasta 64 cámaras IP	
Ancho de banda de entrada:	160Mbps	
Salidas Video:	VGA/HDMI (1920x1080), BNC (704x576)	
E/S Audio:	-/2	
Alarmas E/S:	16/4	
Acceso remoto desde:	software incluido,	

	navegador WEB, iPhone, Android	
IP	Estática o Dinámica	
Puertos	2 x puertos RJ45 (10/100/1000Mbps). 3 x puertos USB. 1 x eSATA. 2 x puertos RS485 (uno para telemetría y otro para teclado)	
Reproducción simultánea	16 canales	
Capacidad de disco duro:	8SATA max 4TB (32 TB)	
Max 128ch remotos simultáneos		
Incluido ratón y mando IR		

Debido a que cada NVR tiene una capacidad de 64 canales IP soportados, se necesita de un equipo adicional de las mismas caracteristicas, para cubrir los 50 Infocentros y 24 Infocentros coon un total de 74 cámaras IP, con los dos equipos tendremos un total de 128 canales, obteniendo una reserva de 54 canales para futuras ampliaciones, sin embargo cada equipo no necesita disponer de todos los discos SATA instalados, para lo cual se realiza el cálculo de la capacidad de almacenamiento requerida para las 74 cámaras, partiendo de la capacidad de almacenamiento requerida para una cámara IP durante un mes de grabación es: 26GB/mes y asumiendo que con la finalidad de equilibrar la capacidad de almacenamiento en cada equipo NVR se relacionan 37 cámaras con cada NVR.

$$26_{GB/mes} * 37_{cámaras} = 962_{GB/mes} = 0{,}96_{TB/mes}$$

Si cada grupo de 25 cámaras que se controlarán con cada NVR necesitan una capacidad en disco de 0,96 TB, teniendo en cuenta que la capacidad mínima de cada disco SATA que se puede incorporar en el NVR es de 4TB, podemos concluir que la instalación de un disco en cada equipo será suficiente para el requerimiento de almacenamiento e incluso se dispone de la opción de incorporar nuevos discos para futuras ampliaciones de capacidad.

5.4.2. Calculo del ancho de banda para VoIP.

Para el cálculo del ancho de banda para una red de VoIP, es importante tomar en consideración los siguientes puntos:

- El número de llamadas concurrentes, se suele denominar de esta manera a la cantidad máxima de llamadas simultáneas que se podrán cursar sobre un enlace. Esta estimación debe considerar tanto la cantidad actual de llamadas telefónicas simultáneas entre diferentes puntos, como el posible margen de crecimiento y las políticas de la organización al respecto.
- El requerimiento de ancho de banda para cursar cada conversación telefónica, cuando se implementa voz sobre IP se asume un conjunto de elecciones que impactan en ese requerimiento: CODEC, opciones de compresión, enlaces sobre los que se rutearán las llamadas, etc.

Para este cálculo se utilizará la siguiente ecuación:

$$C_{canal} = AB_{CODEC} \frac{\text{LONGITUD DE SOBRECARGA} + \text{LONGITUD DE ENCAPSULAMIENTO}}{\text{LONGITUD DE SOBRECARGA}}$$

Ecuación 2

De donde:

C_{CANAL} : Capacidad del canal (bps)
Longitud de sobrecarga: se refiere al tamaño del Payload de la trama.
Longitud de encapsulamiento: tamaño de la cabecera de la trama.

Para el cálculo de la Longitud de encapsulamiento, se suma la dimensión de las cabeceras de los distintos protocolos que intervienen en cada capa del modelo OSI, en la Tabla 5.14, se muestra un detalle del tamaño de las cabeceras de los protocolos utilizados.

Tabla 5. 14 Detalle del tamaño de cabecera de los distintos Protocolos.

NIVEL DE LA CAPA OSI	PROTOCOLO	TAMAÑO DE LA CABECERA
Capa de Sesión	RTP (Real-Time Transport Protocol)	12 Bytes

Capa de Transporte	UDP (Protocolo Datagrama de Usuario)	8 Bytes
Capa de Red	IP Sec (Internet Protocol Security)	20 Bytes
Capa de Enlace de Datos	PPTP (Protocolo de entunelamiento punto a punto)	6 Bytes

$$LONGITUD\ DE\ ENCAPSULAMIENTO = RTP + UDP + IPsec + PPTP$$
$$LONGITUD\ DE\ ENCAPSULAMIENTO = 12\ bytes + 8\ bytes + 20\ bytes + 6\ bytes$$
$$LONGITUD\ DE\ ENCAPSULAMIENTO = 46\ bytes$$

Longitud de sobrecarga = tamaño del payload de la trama, para el Codec G.729 es de 20 Bytes. Ancho de banda que consume el códec G.729 es de 8kbps como lo vimos en la Tabla 8.

$$C_{CANAL} = 8kbps * \frac{20\ bytes + 46\ bytes}{20\ bytes}$$
$$C_{CANAL} = 25.6\ kbps$$

Para el número de llamadas concurrentes se toma en consideración, que en la oficina matriz del MINTEL, hay 6 coordinadores (Analistas técnicos 2) que son los encargados de supervisar el trabajo y asistencia del personal de los Infocentros, por lo que el número de canales o llamadas simultáneas será de 6 y se le adiciona un 30 % para futuro crecimiento, por lo que tenemos un total de 8 canales necesarios.

$$C_{TOTAL} = C_{CANAL} * \#_{CANALES}$$
$$C_{TOTAL} = 25.6\ kbps * 8$$
$$C_{TOTAL} = 204.8\ kbps$$

Los 204,8 kbps es el ancho de banda que se generará un total de 8 llamadas concurrentes en la oficina matriz del MINTEL, sin embargo el ancho de banda que se genera en cada Infocentro o Megainfocentro es el de 25.6 kbps correspondiente al de una llamada.

5.4.3. Cálculo del ancho de banda generado por servicios

El ancho de banda total que se necesita para la implementación de los servicios de video vigilancia y VoIP, dentro de un Infocentro o Megainfocentro está determinado por la suma del consumo de ancho de banda que generan estos dos servicios por separado, siendo:

$$C_{Tred} = C_{video} + C_{voz}$$
$$C_{Tred} = 289{,}65\ K_{bps} + 25.6\ K_{bps}$$
$$C_{Tred} = 315{,}25\ K_{bps}$$

El ancho de banda total que se necesitará para el funcionamiento de estos servicios en la oficina matriz MINTEL, que será en donde se ubique los servidores de VoIP y video, está dado por la suma del consumo de ancho de banda que generan estos servicios por separado, considerando que en la oficina matriz es en donde se recopilará el video de todas las cámaras IP de manera continua durante su operación y se establecerán hasta un máximo de ocho llamadas simultaneas para el control y apoyo de los facilitadores, el consumo total está dado por:

$$C_{Tred(74)} = C_{video(74)} + C_{voz(8)}$$

En donde:

$C_{Tred(74)} =$ Capacidad total de la red generada por los servicios de video y VoIP en los 50 Infocentros y 24 Megainfocentros (74 sitios).

$C_{video(74)} =$ Capacitad total de la red generada por 74 cámaras IP.

$C_{voz(8)} =$ Capacidad total de la red generada por 8 llamadas simultaneas.

$$C_{Tred(74)} = 21{,}4\ M_{bps} + 204{,}8\ K_{bps}$$
$$C_{Tred(74)} = 21{,}4\ M_{bps} + 0{,}20\ M_{bps}$$
$$C_{Tred} = 21{,}6\ M_{bps}$$

5.5. ANÁLISIS DE LAS POLÍTICAS DE QOS SOBRE LA RED DISEÑADA

La calidad de servicio (QoS – Quality of Service).- es el rendimiento de extremo a extremo de los servicios electrónicos tal como lo percibe el usuario final, una red debe garantizar un cierto nivel de calidad de servicio para un nivel de tráfico que sigue ciertos parámetros, para el caso de las redes VPN se refiere al número de conexiones simultáneas o cantidad de túneles que pueden ser establecidos entre un sitio remoto y el sitio Central en una red VPN y la forma como estas afectan al rendimiento de la VPN.

Uno de los principales objetivos de aplicar políticas de calidad de servicio en una red, es la optimización del ancho de banda mediante la priorización del tráfico que curza por dicha red, para analizar cómo se deberán aplicar estas políticas es necesario primero estudiar los siguientes parámetros: [17]

- **Latencia (retardo).-** Es el tiempo que tarda un paquete en llegar desde la fuente al destino, es un problema general de las redes de telecomunicaciones, el retardo de extremo a extremo debe ser inferior a 150 ms, esta recomendación se encuentra ligada a la capacidad auditiva de los humanos que son capaces de detectar retardos de 200 a 250 ms, siempre existirá, ya que está implícito en el tiempo de procesamiento de los equipos de comunicación, pero puede ser controlado.

- **Jitter (la variación del retardo).-** es la variación en el tiempo en la llegada de los paquetes, esto ocurre a causa de: congestión existente en la red, perdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino. Para el jitter se recomienda que tenga un valor menor o igual a 100 ms para tener una comunicación sin molestias, si este parámetro es mayor debe ser minimizado utilizando alguna técnica. [W22]

- **Pérdida de paquetes.-** Este efecto es más suceptible para los servicios que funcionan en tiempo real que hacen uso del protocolo UDP, al no ser un protocolo orientado a conexión una vez que exista pérdida de paquetes, este protocolo no tiene ningún método para reenvío de paquetes, en servicios de vídeo conferencia los efectos de la pérdida de paquetes puede hacer que la imagen sea distorsionada, audio desfasado con respecto a la imagen, se recomienda que la pérdida sea menor de 1%, este parámetro depende del códec que se utilice para el caso de VoIP.

5.5.1. Tipos de tráfico

Fig 5. 23 Clases de Tráficos

- Clase VoIP: requerimientos de BW, pérdida de paquete < 1%, retardo end – to – end < 150ms. Debido a sus altos requerimientos es la clase con mayor prioridad.
- Clase Mission Critical: esta clase se ocupa de las aplicaciones críticas de la empresa o usuario (Transacciones comerciales).
- Clase Tráfico de señalización: Es el tráfico del protocolo SIP para establecimiento de llamadas de VoIP.
- Clase de Aplicaciones Transaccionales: consultas a base de datos y servicios similares.
- Clase BestEffort: todo el tráfico no definido en las clases anteriores caen en esta categoría (se le asigna el BW sobrante).
- Clase Scavenger (Basura): se considera inferior a la clase Best-Effort.

Es necesario determinar las clases de tráfico que vamos a tener en nuestra red, a continuación se realiza un detalle de las mismas:

- Clase VoIP.- En esta clase vamos a incorporar el tráfico del servicio de VoIP propiamente dicho y el tráfico del servicio de video vigilancia, debido a que son tráficos que se manejan en tiempo real, necesitan un bajo porcentaje en pérdida de paquetes, bajo retardo y un gran consumo de ancho de banda.

- Clase tráfico de señalización: tráfico generado por el protocolo SIP, para el servicio de VoIP.
- Clase BestEffort: para el tráfico que se genera por la navegación Web de los usuarios del Infocentro.

5.5.2. Modelos de calidad de servicio

Modelo Best-Effort: Es el modelo por defecto de toda red; no se realiza diferenciación de tráfico por lo que la voz, video y datos tienen la misma prioridad, la red hace lo posible para intentar entregar el paquete a su destino, donde no hay garantía de que esto ocurra, no se aplica ninguna política de QoS. [22]

Servicios Integrados (IntServ): Basado en la reserva de recursos de red para proveer QoS, trabaja con el protocolo RSVP (Resource Resevation Protocol), puede proveer múltiples niveles de servicio, para la implementación de este modelo es necesario activar las siguientes funciones en cada dispositivo de red:

- Control de Admisión: responde al "request" de reserva de recursos de las aplicaciones.
- Clasificación: tráfico perteneciente a una aplicación con reserva de recursos debe ser clasificado y reconocido.
- Vigilancia (Policing) : monitoreo para que aplicaciones no excedan la utilización de los recursos reservados
- Queuing: mecanismos de encolamiento dan diferente tratamiento a los datos.
- Planificador (Scheduling): existencia de varios queues en una misma interfaz necesitan de un planificador.

Al ser un modelo basado en flujos, no es escalable para implementaciones a gran escala como en Internet.

Servicios Diferenciados (DiffServ): Este modelo incluye un conjunto de herramientas de clasificación del tipo de tráfico y mecanismos de cola para aplicaciones con prioridades sobre el resto del tráfico en la red. El tráfico de red puede ser clasificado por: dirección de red, protocolo, puertos, interfaz de ingreso o cualquier tipo de clasificación que pueda ser alcanzada mediante el uso de listas de acceso. [22]

5.5.3. Métodos de implementación de Calidad de Servicio

Como estamos trabajando con equipos CISCO, entonces debemos hacer referencia a los cuatro métodos de implementación de calidad de Servicio para esta tecnología, estos son:

- Método CLI (Command Line Interface)
- Método MQC (Modular QoS CLI)
- AutoQoS
- SDM (Security Device Manager) QoS Wizard

5.5.3.1. Método CLI (Command Line Interface)

El método Command Line Interface es el método más antiguo para configurar QoS en dispositivos de red CISCO, su configuración se la realiza a través de varias líneas de código, y cada interface deberá ser configurada de forma separada lo que le convierte en un método poco eficiente y más susceptible de errores, requiere de tres pasos para su aplicación:

- Identificación, clasificación y priorización de tráfico
- Seleccionar una de las herramientas de QoS disponibles (Queuing, compresión)
- Aplicar los mecanismos de QoS a la interfaz

5.5.3.2. Método MQC (Modular QoS CLI)

Se puede decir que es la evolución del método CLI, la clasificación de tráfico y la definición de políticas se las realiza de manera separada, es un método más eficiente y consume menos tiempo de procesamiento, de igual manera su aplicación se basa en tres pasos:

- Mapa de clase (class map), se definen las clases de tráfico
- Mapa de política (policymap), se especifica los parámetros de QoS que se aplicarán a una clase de tráfico
- Política de servicio, aplica el (policymap) que contiene las políticas de QoS a una interfaz determinada.

5.5.3.3. Método CISCO (Auto QoS)

Esa herramienta lo poseen los equipos CISCO, esta herramienta genera automáticamente class-maps (clases de tráfico) y policy-maps (Políticas de QoS), es de gran ayuda para aplicaciones de gran escala en las que la aplicación de políticas a cada interfaz resulta un trabajo laborioso, realiza la clasificación de tráfico a través de NBAR, su configuración es muy sencilla, depende de los siguientes pasos: [W23]

- Habilitar CEF(Cisco Express Forwarding)en la interfaz
- Habilitar NBAR(Network Based Application Recognition) en la interfaz
- Configuración del ancho de banda en la interfaz
- Aplicar el comando auto QoS en la interfaz

Debido al número de equipos que se necesitan configurar y la distancia geográfica a la que se encuentran cada uno de ellos, se optará por el método Auto QoS para la aplicación de calidad de servicio en la red VPN y deberá ser aplicado en los routers CISCO de cada Infocentro o Megainfocentro así como también en el router de la oficina matriz del MINTEL.

5. CONCLUSIONES

- El proyecto Ampliación de la Red Infocentros, ha implementado a nivel nacional un total de 267 Infocentros y 24 Megainfocentros; de este total se seleccionaron para este estudio 50 Infocentros y 24 Infocentros que disponen del servicio de internet a través de Fibra Óptica por disponer de velocidades de transmisión favorables para la implementación de los sistemas de videovigilancia y VoIP.

- El diseño del sistema de video vigilancia de cada Infocentro, contempla una cámara IP por cada Infocentro o Megainfocentro, con un total de 74 cámaras Web, configuradas en modo detección de movimiento, con la finalidad de reducir los tiempos muertos de grabación y manejar de manera eficiente el espacio en los discos de almacenamiento.

- Para la elección de las cámaras web a ser instaladas se tomaron en cuenta parámetros que aporten a un ahorro en el consumo de ancho de banda de la red, pero que brinden una buena calidad de imagen: resolución 4CIF NTSC, 5 Ips, estándar de compresión MPEG-4.

- Para el sistema de VoIP se considera el uso del Codec de voz G.729 ya que posee una buena calidad en la conversación con un mínimo consumo de ancho de banda, el costo del pago se licencia por número de canales simultáneos, se justifica en el aprovechamiento del ancho de banda y en la calidad de la voz.

- Para el cálculo del ancho de banda requerido para el funcionamiento del sistema de video vigilancia y VoIP, se considera que cada Infocentro o Megainfocentro deberá contar con una cámara IP y un teléfono IP que estarán conectados a la red del Infocentro y tendrán comunicación con la oficina central de MINTEL a través de una red VPN de tipo intranet.

- La calidad de servicio se la aplica con la aplicación del Método Auto QoS, que disponen los equipos CISCOS, para esto se ha tomado en cuenta el número de interfaces que se necesitan configurar, además de la ubicación geográfica en la que se encuentran los Infocentros y Megainfocentros.

6. RECOMENDACIONES

- Se recomienda al Proyecto Ampliación de la Red Infocentros, realizar un estudio de disponibilidad del servicio de Internet a través de Fibra Óptica, de modo que se pueda determinar el número de Infocentros que pueden migrar de las tecnologías ADSL, VSAT hacia la tecnología Fibra Óptica, para ofrecer Internet a mayor velocidad y con los servicios de VoIP y video vigilancia IP.

- Para la configuración de las cámaras IP, se recomienda que estas sean programadas para un máximo de captura de 5 imágenes por segundo, ya que nos permite reducir el consumo de ancho de banda con una calidad de imagen aceptable, perceptible al ojo humano.

- Para reducir el ancho de banda que consume el servicio de VoIP, así como también la cantidad de pérdida de paquetes, se recomienda que los terminales IP utilizados en para VoIP, dispongan de la característica Voice Activity Detection, que impide la transmisión de los tiempos de silencio.

- Se recomienda la aplicación de políticas de calidad de servicio a la red VPN, de modo que la red ser capaz de identificar y asegurar los distintos tráficos y otorgarles un tratamiento específico para los servicios: VoIP, video, navegación WEB.

- Se recomienda la incorporación de algún software de monitoreo de red, con el fin de controlar el consumo del ancho de banda y detección de fallas que permitan tomar acciones correctivas antes de que implique un problema para los servicios que los Infocentros y Megainfocentros brindan a la ciudadanía, además que la aplicación de un monitor de red contribuye a mejorar la calidad de servicio de la red.

7. BIBLIOGRAFIA

[1] Constitución de la República del Ecuador, Registro Oficial 449 de 20-oct-2008.

[2] Información del Proyecto, Convenio CNV-0756-2013.

[3] Plan Nacional del Buen Vivir, Secretaría de Planificación y Desarrollo, ISBN-978-9942-07-448-5, 2013-2017.

[4] Ministerio de Telecomunicaciones y de la Sociedad de la Información, Planificación estratégica MINTEL 2016.

[5] Segunda Adenda al Convenio CNV 0756-2013, MINTEL-CNT EP, Especificaciones Técnicas

[6] Arturo B. Grandón, "Vigilancia mediante video IP, Videovigilancia IP", 2008.

[7] Silvia M. Martí, "Diseño de un sistema de televigilancia sobre IP para el edificio CRAI de la Escuela Politécnica Superior de Gandia", Universidad Politécnica de Valencia, 2003.

[8] Jumbi Edulbehram, Eric Fullerton, Una forma más inteligente de proteger su comercio: la videovigilancia IP, AXIS Comunicatios, 2008.

[9] IRONTEC Internet y sistemas sobre GNU/Linux, "Introducción a la VoIP y Asterisk.

[10] Edgar Landívar, "Comunicaciones Unificadas con Elastix", volumen 1, 2008.

[11] Bob Fryer, Trunking between two Elastix PBX Systems Via VPN, 2011.

[12] Diego Quintana Cruz, "Diseño e implementación de una red de telefonía IP con software libre en la RAAP", Pontificia Universidad Católica del Perú, 2007.

[13] Jose Luis Ruiz González, VPN - Redes Privadas Virtuales, 2002.

[14] Edgar Arturo Bustos Caldas, Componentes básicos para una red segura bajo VPN, Revista Inventum No. 3, 2007.

[15] Santiago Pérez Iglesias, Análisis del protocolo IPSec: el estándar de seguridad en IP, 2001.

[16] Alexandro González Morales, Redes Privadas Virtuales, Universidad Autónoma del Estado de Hidalgo, 2006.

[17] Flavio N. Carrillo, Anderson Calderón, Parámetros de calidad de Servicio en redes IP, Universidad Mayor de San Marcos, 2008.

[18] Sebastián A. Álvarez, Agustín J. González, "Estudio y configuración de calidad de servicio para protocolos IPv4 e IPv6 en una red de fibra óptica WDM", 2005.

[19] Morelis Gonzalo Vega, "Los Infocentros venezolanos ¿un esfuerzo de inclusión social?", Universidad de Zulia, 2005.

[20] AXIS COMUNICATIONS, Guía Técnica de video IP, Factores y Técnicas a considerar para un correcto uso de las aplicaciones de vigilancia y monitorización remotas basadas en IP.

[21] Wilmer Santamaría Gonzales, Protocolos de señalización usada actualmente para terminales móviles e IP, KONRAD LORENTZ, 2011.

[22] Sebastián Andrés Álvarez Moraga, Estudio y Configuración de Calidad de Servicio para Protocolos Ipv4 e Ipv6 en una Red de Fibra Óptica WDM, 2005.

8. WEBGRAFÍA

[W1] Securame videovigilancia y seguridad, cámaras IP, http://www.securame.com/domo-ip-hikvision-ds2cd793pfe-ccd-13-704x576-25fps-h264-2811mm-002lux-sd-poe-antivandalica-p-1031.html

[W2] CISCO, Voz sobre IP información básica, http://www.cisco.com/web/ES/solutions/es/voice_over_ip/index.html

[W3] Handley M, Schulzrinne H, et al. 'SIP: Session Initiation Protocol'. 1999. URL: http://www.ietf.org/rfc/rfc2543.txt.

[W4] CISCO, Voz sobre IP - Consumo de ancho de banda por llamada, http://www.cisco.com/cisco/web/support/LA/7/73/73295_bwidth_consume.pdf

[W5] POLYCOM, Teléfono IP VVX 201, http://www.polycom.com/products-services/voice/desktop-solutions/realpresence-desktop-vvx-business-media-phones/vvx-201.html

[W6] YEALINK, Teléfono IP SIP-T9, http://yealink.com/product_info.aspx?ProductsCateID=334

[W7] CISCO, Teléfono IP SPA502G, http://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/small-business-spa500-series-ip-phones/data_sheet_c78-548561.pdf

[W8] PANASONIC, Teléfono IP KX-HDV130, http://panasonic.net/pcc/products/sipphone/products/kx_hdv130/specifications.html

[W9] CISCO, RV082 Dual WAN VPN Router http://www.cisco.com/c/en/us/products/collateral/routers/rv082-dual-wan-vpn-router/data_sheet_c78-501227.pdf

[W10] CISCO, Router C881 Datos técnicos, http://www.cisco.com/c/en/us/support/routers/c881-integrated-services-router/model.html#~tab-documents

[W11] HIKVISION, IP NVR recorder 64 channels DS-9664NI-ST, http://www.bkeesti.ee/en/tooted/hikvision-ip-nvr-recorder-64-channels-ds-9664ni-st/

[W12] MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN, Definición de Infocentros, http://www.telecomunicaciones.gob.ec/infocentros-comunitarios/

[W13] SOLUCIONES SIEMPRE, Evolución de los sistemas CCTV, http://www.solucionessiempre.mx/?p=699

[W14] AXIS COMUNICATIONS, Video Compression, http://www.axis.com/es/es/learning/web-articles/technical-guide-to-network-video/compression-formats

[W15] AXIS COMUNICATIONS, Resoluciones, http://www.axis.com/co/es/learning/web-articles/technical-guide-to-network-video/resolutions.

[W16] Universidad Nacional Abierta y a Distancia, Protocolo SIP, http://datateca.unad.edu.co/contenidos/299009/299009-2015/eXelearning/Modulo/leccin__11.html

[W17] ELASTIXTECH, Protocolo IAX, http://elastixtech.com/protocolo-iax/

[W18] 3CX, Qué significa los términos FXS y FXO, http://www.3cx.es/voip-sip/fxs-fxo/

[W19] CISCO, Cómo funcionan las redes privadas virtuales, http://www.cisco.com/cisco/web/support/LA/7/74/74718_how_vpn_works.pdf

[W20] MICROSOFT, Protocolo de tunel punto a punto, https://msdn.microsoft.com/es-es/library/cc739465%28v=ws.10%29.aspx

[W21] MICROSOFT, Protocolos de tunel VPN, https://technet.microsoft.com/es-es/library/cc771298%28v=ws.10%29.aspx

[W22] ELASTIXTECH, QoS-Calidad de Servicio para VoIP, http://elastixtech.com/qos-calidad-de-servicio-para-voip/

[W23] CISCO, Implementación de Soluciones QoS para Videoconferencia H.323 sobre IP, http://www.cisco.com/cisco/web/support/LA/102/1026/1026685_video-qos.pdf