

UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA



**ESTUDIO, DISEÑO Y COSTOS DE UNA RED DE
TELECOMUNICACIONES EN UNA EMPRESA CORPORATIVA**

**INFORME DE COMPETENCIA PROFESIONAL
PARA OPTAR EL TÍTULO PROFESIONAL DE:
INGENIERO DE TELECOMUNICACIONES**

**PRESENTADO POR:
LUIS ENRIQUE ZAMBRANO TORRES**

**PROMOCIÓN
2006 – II**

**LIMA – PERÚ
2014**

**ESTUDIO, DISEÑO Y COSTOS DE UNA RED DE
TELECOMUNICACIONES EN UNA EMPRESA CORPORATIVA**

Dedicatoria:

Dedico la realización de este informe a mis padres y a mi hermano por todo su apoyo y comprensión para el cumplimiento de este objetivo.

SUMARIO

En el presente informe se realiza el estudio de una red de telecomunicaciones de una empresa peruana que se dedica a la fabricación y venta de productos de belleza, esta red brinda principalmente servicios de datos y telefonía a los usuarios que laboran en la compañía.

La empresa cuenta con varias oficinas funcionando en la ciudad de Lima; las consideraciones para el diseño deben hacer que la red de telecomunicaciones sea escalable y que en un futuro soporte la demanda de nuevas tecnologías; por otro lado la red es redundante a todo nivel lo cual garantiza la continuidad de los servicios de telecomunicaciones que la red brinda a los usuarios.

Luego de realizar el diseño de la red, se procede con la cuantificación del equipamiento de telecomunicaciones a fin de obtener la cantidad de equipos empleados en la implementación.

En la última parte del informe se muestran los costos por concepto de, implementación, operación y mantenimiento de la red de telecomunicaciones.

ÍNDICE

Página

CAPÍTULO I	1
INTRODUCCIÓN	1
CAPÍTULO II	3
MARCO TEÓRICO	3
2.1. Topología de red.....	3
2.1.1. Topología Física.....	3
2.1.2. Topología Lógica.....	4
2.2. Tecnologías Ethernet e IEEE 802.3	5
2.2.1. Tipos de Ethernet.....	7
2.2.2. Conmutación en Ethernet.....	8
2.3. Modelo TCP/IP	12
2.3.1. Protocolo de Internet (IP).....	12
2.3.2. Protocolo de datagrama de Usuario - UDP	15
2.3.3. Protocolo de control de la transmisión - TCP.....	17
2.4. Tecnología voz sobre IP – VoIP	19
2.4.1. Funcionamiento de la voz sobre IP.....	19
2.4.2. Protocolo H.323.....	20
2.4.3. Conjunto de protocolos H.323	23
2.5. Tecnología de conexión punto a punto	25
2.5.1. Conexión de dos puntos por intermedio de fibra óptica.	25
2.5.2. Conexión de dos puntos por intermedio de un radio enlace.....	26
2.5.3. Conexión de dos puntos por intermedio de la red de un tercero.	27
2.6. Calidad de servicio	27
2.6.1. Tipos de calidad de servicio.....	28
2.6.2. Formación de anillos	29
2.6.3. Reservación de ancho de banda (RSVP)	29
2.7. Seguridad de la información	30

2.7.1	Seguridad perimetral	31
2.7.2.	Seguridad dentro de la LAN.....	32
2.7.3.	Tecnología de prevención de ataques	33
CAPÍTULO III		35
DETERMINACIÓN DE NECESIDAD		35
3.1.	Servicios a Prestar.....	35
3.2.	Cálculo de la demanda	35
3.2.1.	Consideraciones previas al cálculo de la demanda	36
3.2.2.	Consideraciones previas de diseño.....	38
3.2.3.	Cálculo de la demanda de datos.....	40
3.2.4.	Cálculo de la demanda de líneas telefónicas externas	46
3.3.	Interconexión de servicios con la red externa.....	47
3.3.1.	Servicios externos – Datos.....	48
3.3.2.	Servicios externos – Voz	50
3.3.3.	Interconexión de sedes secundarias y remotas.....	51
CAPÍTULO IV		54
INGENIERÍA DEL PROYECTO		54
4.1.	Estructura de la red corporativa	54
4.1.1.	Capacidad de los switches de acceso.....	55
4.1.2.	Capacidad de los switches de núcleo	58
4.1.3.	Red de acceso	63
4.1.4.	Otro tipo de redes de acceso.....	65
4.1.5	Detalle de diseño	73
4.2.	Dimensionamiento del proyecto	79
4.2.1.	Dimensionamiento de los switches.....	79
4.2.2.	Dimensionamiento de la solución de telefonía IP.....	80
4.2.3.	Dimensionamiento de la seguridad perimetral.....	80
4.3.	Especificaciones técnicas.....	80
4.3.1.	Especificaciones técnicas de los switches	80
4.3.2.	Especificaciones técnicas de los equipos de telefonía IP.....	82
4.3.3.	Especificaciones técnicas del equipo de seguridad perimetral	83
4.4.	Subsistema de energía y protección eléctrica.....	83

CAPÍTULO V	88
COSTO DEL PROYECTO	88
5.1. Costos de inversión de implementación.....	88
5.1.1. Costo por compra equipos propios	88
5.1.2. Costo por instalación y configuración de equipos propios	89
5.1.3. Costo por instalación de servicios arrendados	89
5.2. Costos de operación y mantenimiento	90
5.2.1. Costos de operación.....	90
5.2.2. Costo por mantenimiento de equipos propios.....	91
CONCLUSIONES Y RECOMENDACIONES	93
GLOSARIO DE TÉRMINOS	95
ANEXO A	97
BIBLIOGRAFÍA	101

CAPÍTULO I INTRODUCCIÓN

El siguiente informe es un estudio de la infraestructura de la red de telecomunicaciones de una empresa peruana dedicada a la elaboración y venta de productos de belleza, la cual brinda a los usuarios servicios de telecomunicaciones para el desarrollo de sus actividades diarias.

Los usuarios de las redes corporativas cada día requieren mayor y mejor rendimiento en sus actividades laborales, esto conlleva a que la red de telecomunicaciones debe estar preparada para soportar no solo los servicios tradicionales como son la navegación a internet, telefonía IP o el correo electrónico, sino también que tengan la capacidad de brindar servicios más colaborativos al usuario.

En el siguiente estudio se muestra una red de telecomunicaciones con alta disponibilidad, que permite a los usuarios acceder a su información y servicios de manera confiable, asimismo que soporte futuros servicios que demanden mayores recursos en la red.

La empresa objeto de estudio cuenta con varias oficinas en la ciudad de Lima, la sede principal es el centro de operaciones de la empresa y cuenta con la mayor cantidad de usuarios, por tal motivo la continuidad de los servicios de telecomunicaciones para la sede principal es un factor primordial.

En la segunda parte del informe se muestra los conceptos teóricos que sirven como fundamento de las tecnologías empleadas en la red de telecomunicaciones, se muestra además las tecnologías que se usan actualmente para el aseguramiento de la información dentro de una red de datos.

En la tercera parte del informe se determinan las necesidades de los usuarios dentro de la empresa y en base a eso se dimensionan los servicios de telecomunicaciones brindados, el dimensionamiento se realiza con una proyección de crecimiento a cinco años, además se muestra la forma como algunos servicios internos interactúan con servicios que están fuera de la red de manera confiable y segura.

En la cuarta parte del informe se muestra el diseño de la red con las consideraciones que aseguran alta disponibilidad en los servicios; además se calcula la cantidad de equipos de telecomunicaciones empleados en la implementación y se listan las características técnicas que deben cumplir.

La quinta parte del informe muestra el costo de inversión e implementación de la red de

telecomunicaciones, además se calcula el valor del costo por operación y mantenimiento de la red implementada.

En la última parte del informe se indican las conclusiones y recomendaciones obtenidas del presente estudio.

CAPÍTULO II MARCO TEÓRICO

Una red de telecomunicaciones es un conjunto de equipos interconectados entre sí que permite la transmisión de información a través de ella de forma confiable; de acuerdo a su área de acción se clasifican de la siguiente manera:

- LAN: Red de área local, es una red de uso privado, el área de acción para esta red es el correspondiente a una empresa, un colegio o una universidad.
- MAN: Red de área metropolitana, esta es una terminología que cada vez se usa menos pero busca hacer referencia a redes implementadas sobre un área más extensa que una LAN a nivel de una ciudad por ejemplo.
- WAN: Red de área amplia, el área de acción para una red WAN como su nombre indica puede ser de un área geográfica muy extensa, a nivel de un país o de toda una región.

2.1. Topología de red

La topología de una red se clasifica en topología física y topología lógica.

2.1.1. Topología Física

De acuerdo a su disposición tenemos lo siguiente:

- Topología de bus: Es una topología de fácil implementación y bajo costo, tiene como desventaja que una falla dentro de la red afectaría a todos los usuarios que están en ella.
- Topología de anillo: A diferencia de una topología de bus, en este tipo de arreglo no existe una estación de inicio y fin, físicamente tienen una disposición cerrada.
- Topología de estrella y estrella extendida: Esta es una de las topologías más usadas en las redes LAN, en esta topología cada estación está conectado al nodo central (Switch) a través de su propio cable, lo cual ante una falla en alguno de estos cables solo afecta a la estación directamente conectada.
- Topología de malla completa y de semi-malla: La finalidad de este tipo de topología es obtener una red tolerable a los fallos sin interrumpir los servicios que soporta, esto lo hace a través de múltiples enlaces entre los equipos de comunicaciones.

- Topología Jerárquica: Es similar a una topología de estrella pero el nodo central no tiene todos los nodos conectados, sino que ahora sería un nodo principal el cual solo tiene una cantidad determinada de nodos conectados y estos a su vez conectan mas nodos.
- Topología Mixta: En la práctica una red no solo adopta alguna de las topologías indicadas anteriormente, podría adoptar otras o podría tener más de una topología implementada a la vez, este último escenario es el más común para la mayoría de redes LAN, MAN o WAN.

En la figura 2.1 se muestra los diferentes tipos de topologías físicas.

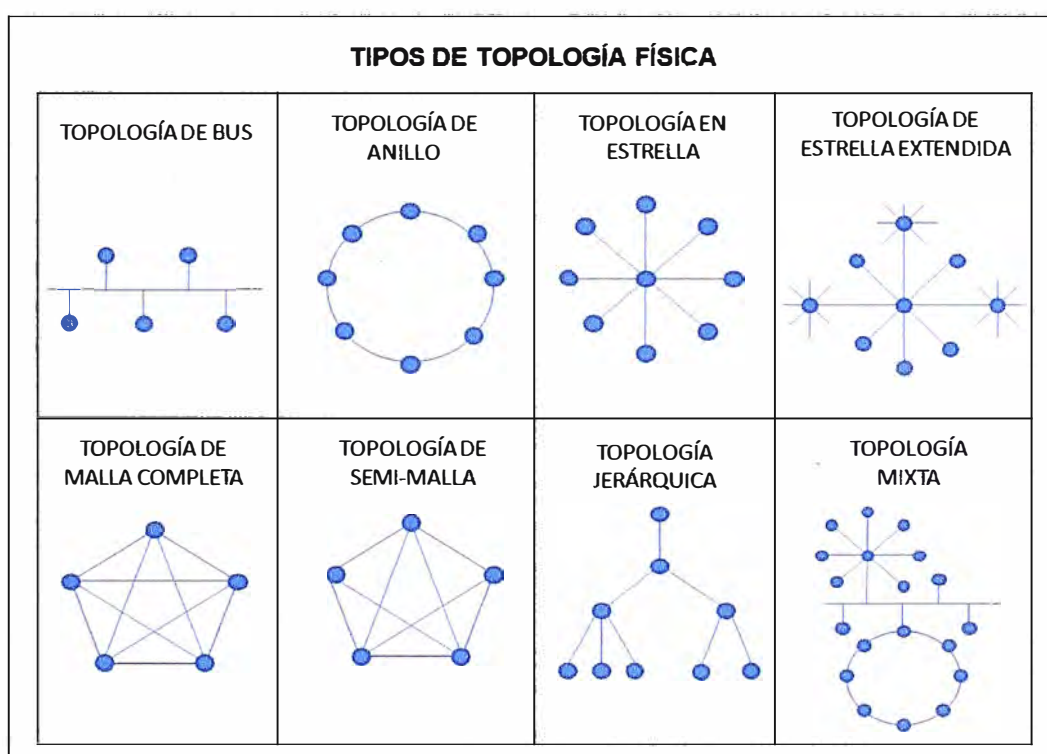


Figura 2.1 Tipos de Topología Física

2.1.2. Topología Lógica

La topología lógica hace referencia a la forma en la cual los dispositivos de la red se comunican a través de un medio físico, las principales topologías lógicas son la de difusión y la de transmisión de testigo.

- Difusión: Esta es la forma para la transmisión de datos de la tecnología Ethernet, en la figura 2.2 se muestra las formas que tiene una estación para transmitir datos.

La transmisión Unicast realiza la difusión de los datos a una estación en particular; la transmisión Multicast realiza la difusión de los datos a un grupo particular de estaciones y la transmisión Broadcast ocurre cuando se realiza difusión de datos a todas las estaciones de la red.

- Transmisión de testigo: El acceso de la red se realiza a través del uso de un testigo electrónico que pasa por cada una de las estaciones en la red, si una estación desea realizar una transmisión de datos debe esperar tener el testigo electrónico para poder hacerlo, en caso no realice ninguna transmisión solo deja pasar el testigo a la siguiente estación. Las tecnologías de acceso que usan este tipo de transmisión son las de Token Ring y FDDI sobre una topología física de anillo.

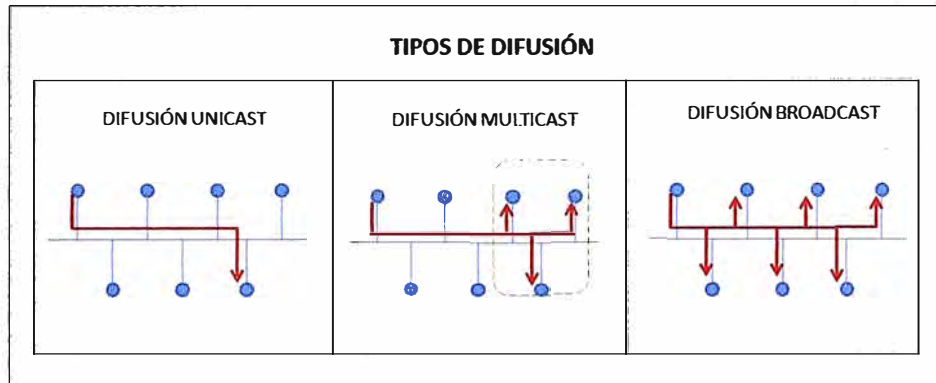


Figura 2.2 Tipos de difusión

2.2. Tecnologías Ethernet e IEEE 802.3

Ethernet usa el método de acceso al medio denominado CSMA/CD, bajo este método de acceso cualquier estación de la red que desee acceder al medio debe previamente verificar que no exista otra estación transmitiendo en la red y que el medio este libre.

Cuando dos estaciones transmiten al mismo tiempo se produce una colisión, en ese momento ambas estaciones continúan transmitiendo por un periodo adicional a fin que las demás estaciones escuchen y sepan que el medio está ocupado, luego todas las estaciones dejan pasar un tiempo aleatorio y vuelven a escuchar el medio a fin de transmitir sus tramas, en la figura 2.3 se muestra la colisión en la transmisión de paquetes de dos equipos dentro de un dominio de colisión.

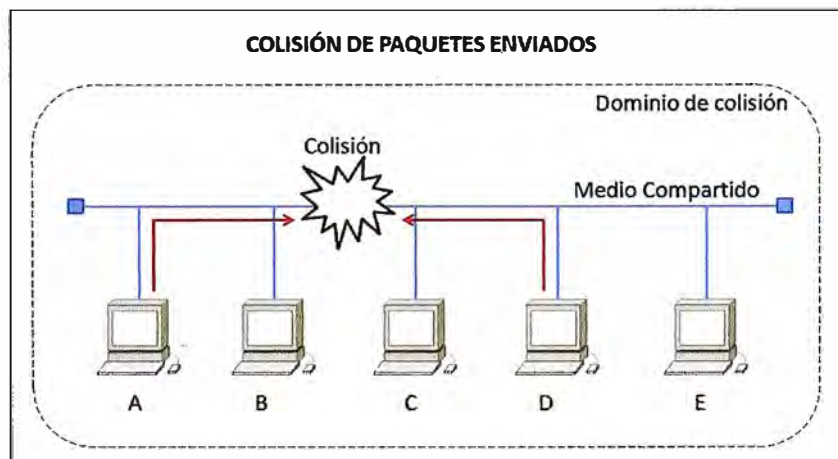


Figura 2.3 Colisión de paquetes enviados

Si bien es cierto que las normas IEEE 802.3 se basaron en gran parte de la tecnología Ethernet existen algunas diferencias entre ambas, por ejemplo Ethernet trabaja específicamente en las capas Físicas y de Enlace de datos del modelo OSI a diferencia de las normas IEEE 802.3 que especifica funciones en la capa física y en una porción de la capa de enlace de datos. En la figura 2.4 se muestra esta diferencia.

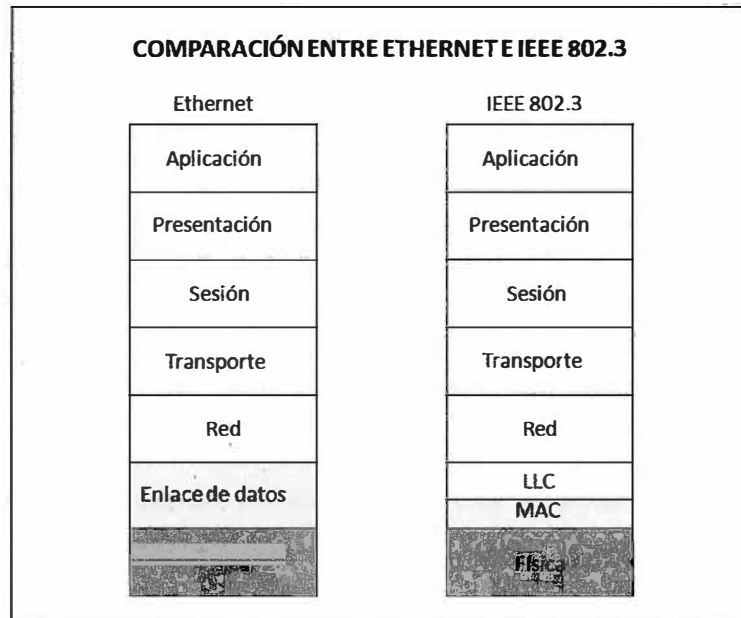


Figura 2.4 Comparación entre Ethernet e IEEE 802.3

La subcapa inferior de control de acceso al medio (MAC), como su nombre lo indica especifica la forma como las estaciones dentro de la LAN se conectarán a la red.

La subcapa superior de control de enlace lógico (LLC), sirve como una interfaz para la comunicación con los protocolos de las capas superiores, en la figura 2.5 se muestra la estructura de la trama de ambas tecnologías.

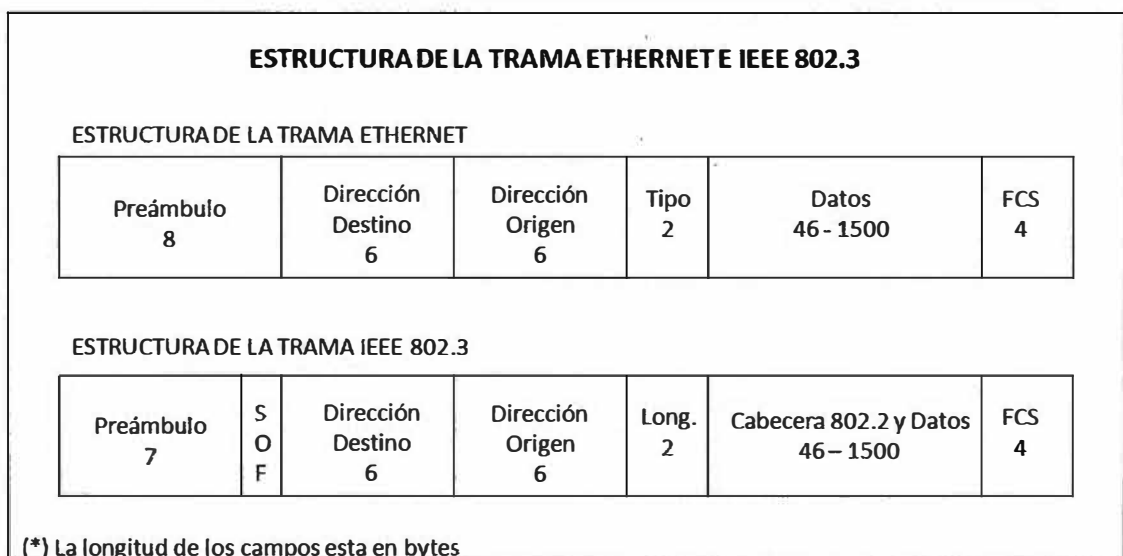


Figura 2.5 Estructura de la trama Ethernet e IEEE 802.3

- **Preámbulo:** Es una secuencia alternada de unos y ceros que indica a las demás estaciones que una trama está por venir, en Ethernet incluye un byte adicional que es el equivalente al SOF de la norma IEEE.
- **Inicio de trama (SOF):** Es una secuencia de unos y ceros en un byte de la siguiente forma 10101011, los dos últimos unos ayudan a la sincronización de la trama con las demás estaciones, este último byte esta adicionado de manera específica en Ethernet.
- **Dirección destino y dirección origen:** Indican entre quienes se da la comunicación, la dirección de origen siempre es unicast, mientras que la dirección destino puede ser unicast, multicast o broadcast.
- **Tipo (Ethernet):** Indica el protocolo de capa superior que recibe la data luego de que el proceso de Ethernet es terminado.
- **Longitud (IEEE):** Indica la cantidad de bytes que tiene el campo de datos a continuación.
- **Datos (Ethernet):** Luego que Ethernet le da tratamiento a la trama desde la capa física hasta la capa de enlace de datos la data se encuentra lista para ser enviada a la capa superior de acuerdo al protocolo definido en el campo correspondiente, con respecto al tamaño de data Ethernet espera por lo menos recibir 46 bytes de data.
- **Datos (IEEE 802.3):** Luego del tratamiento de la data a través de la capa física y de enlace de datos, la data es enviada a la capa superior de acuerdo al protocolo definido dentro de la misma data, para este campo se espera como mínimo 64 bytes, de no alcanzarlo se introducirán bytes a fin de asegurar el mínimo de bytes esperados.
- **Secuencia de revisión de trama (FCS):** consta de una revisión redundante cíclica de 4 bytes, la cual es calculada por el dispositivo que envía la trama y luego recalculada por el dispositivo que la recibe a fin de revisar que no haya habido errores durante la transmisión.

2.2.1. Tipos de Ethernet

- **Ethernet 100BASE – Tx:** Este tipo de Ethernet usa como medio de transmisión los cables UTP de categoría 5 o superior, para la transmisión o recepción de datos usa solamente dos pares de hilos de los 4 pares disponibles, para obtener 100 Mbps la codificación usada en los dos pares de hilos es la 4B/5B.
Este tipo de Ethernet de 100 Mbps tuvo gran aceptación y su uso fue cada vez más frecuente hasta la actualidad, donde su implementación es mayoritaria.
- **Ethernet 1000BASE –T** - Es la tecnología desarrollada para cables UTP cat5e o superior, está desarrollado con una sofisticada tecnología que le permite usar los 4 pares de hilos de cobre para que transmitan y reciban información al mismo tiempo. Esta tecnología es 10 veces más rápida que su antecesora por lo que los tiempos de bit

también se reducen en una décima parte, esto hace que la temporización y sincronización de los datos sea más crítica que en tecnologías anteriores, además el envío de información es mayor y con mayor frecuencia; usa codificaciones diferentes a las tecnologías anteriores.

El hecho que los cuatro pares de hilos transmitan y reciban información al mismo tiempo hace que los niveles de voltaje sean muy variados y muy complejos, motivo por el cual el tratamiento de estos niveles de voltaje debe ser muy cuidadoso a través de una electrónica compleja.

- **1000BASE-SX y 1000BASE-LX** - Estas tecnologías emplean como medio de transmisión de datos la fibra óptica, lo cual permite obtener características diferentes en la transmisión, como son distancia, inmunidad al ruido, etc. Debido a su inmunidad a las diferencias de potencial con la conexión de tierra, estas tecnologías son usadas como backbone para la conexión entre equipos de comunicaciones, switches y routers.

Ethernet 1000 Mbps sobre fibra óptica usa una codificación 8B/10B convertida a codificación de línea NRZ, esto se envía mediante haces de fuentes de laser y dependiendo de la longitud de onda de estos haces de luz se obtendrán diferentes resultados en lo que se refiere a distancia.

1000BASE-SX esta especificada para fibras multimodo, mientras que 1000BASE-LX está adaptada tanto para fibra multimodo como monomodo.

- **10 Gbps Ethernet:** Es el más reciente y más rápido de los estándares Ethernet. Se especifica en el estándar IEEE 802.3ae que lo define como una versión de Ethernet con una velocidad nominal de 10 Gbps, actualmente permite conexiones tanto en fibra óptica como con cable de cobre (UTP cat. 7).

2.2.2. Conmutación en Ethernet

Los switches son utilizados en la implementación de redes LAN, la mayoría de los switches emplean la tecnología Ethernet.

En Ethernet la conmutación se realiza mediante el uso de una tabla de direcciones MAC, que vincula las direcciones MAC con los puertos del equipo switch.

Un switch recién encendido no tiene información sobre las estaciones que tiene conectado en cada uno de sus puertos, por lo que atiende todas las transmisiones que se generan dentro del switch anotando a través de qué puerto entra cada dirección MAC de origen, en la figura 2.6 se muestra el estado inicial de una tabla MAC de un switch recién encendido. A fin de conocer que dispositivos tiene conectado en cada uno de sus puertos el switch enviará la transmisión a todos sus puertos con excepción del puerto por el cual recibe la información, de esta manera podrá averiguar el puerto en el que se encuentra la estación de destino y podrá completar su tabla MAC. este concepto lleva por nombre inundación

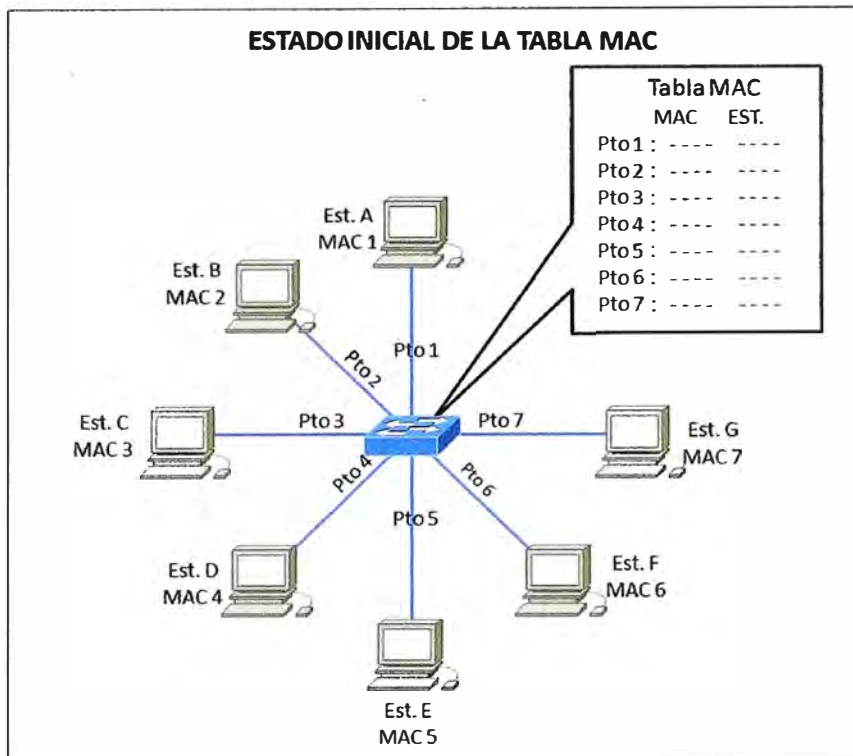


Figura 2.6 Estado inicial de la tabla MAC

Por ejemplo si la estación C conectada al puerto 3, desea transmitir una trama a la estación F que se encuentra conectada en el puerto 6, el switch ingresa la dirección MAC de origen a través del puerto 3 por donde la recibe, en la figura 2.7 se muestra el envío de información de la estación C a la estación F en un switch que tiene su tabla MAC en blanco.

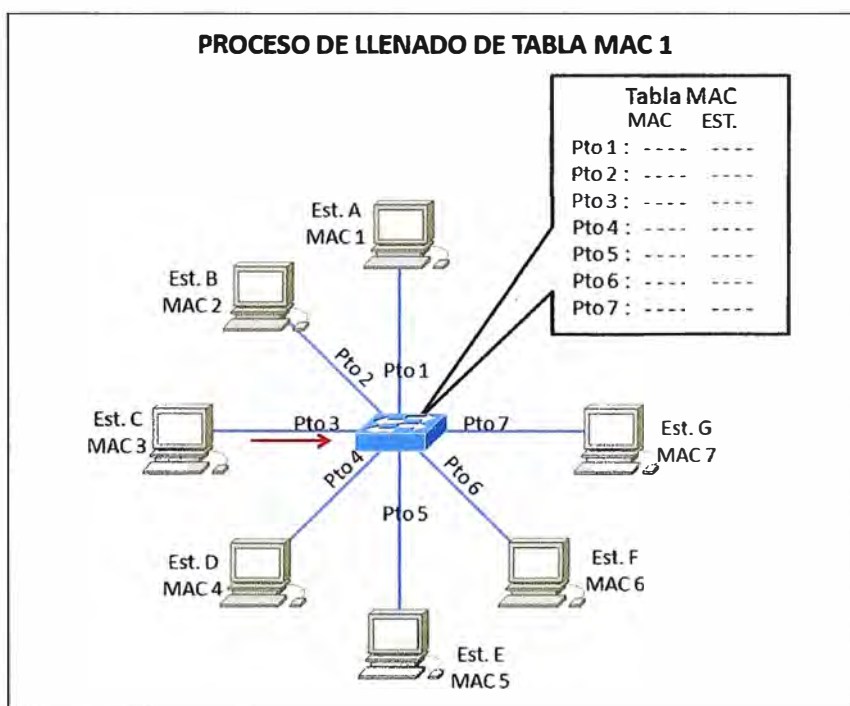


Figura 2.7 Proceso de llenado de tabla MAC 1

El switch aprende que por el puerto 3 tiene conectado la estación C pero como aun no conoce la dirección de destino envía el mensaje por todos los puertos a excepción del puerto origen, en la figura 2.8 se muestra el proceso realizado por el switch.

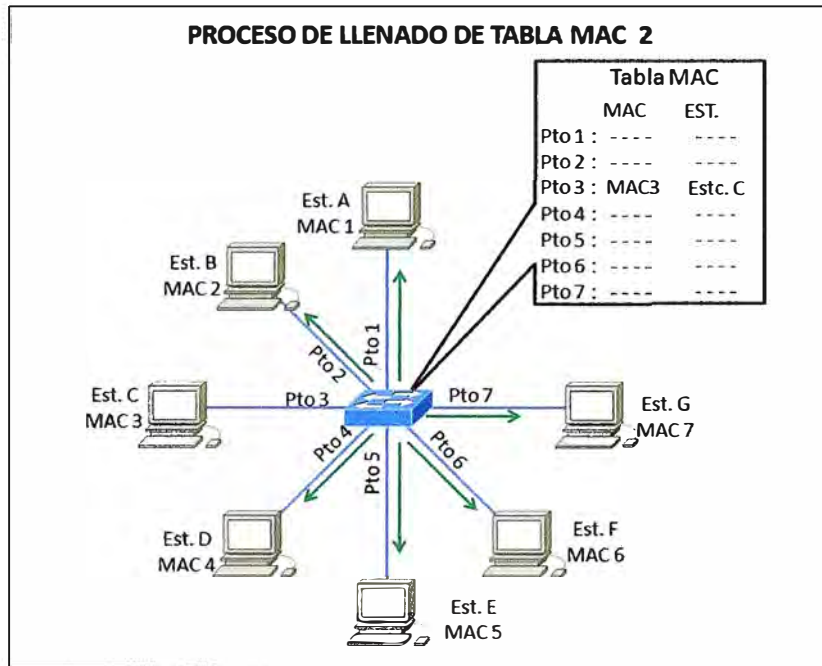


Figura 2.8 Proceso de llenado de tabla MAC 2

Luego de que todas las estaciones reciben la trama y la procesan, la estación F responde, de modo que el Switch añade su dirección MAC en su tabla, en la figura 2.9 se muestra la respuesta de la estación F.

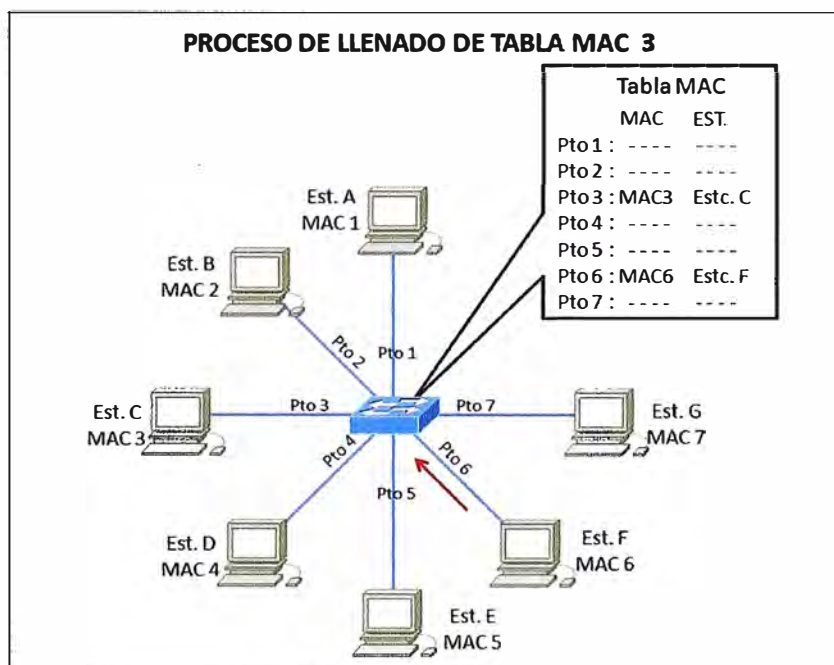


Figura 2.9 Proceso de llenado de tabla MAC 3

Luego el switch recibe la trama y la envía a través del puerto 3 hacia la estación C, de esta manera el switch conoce en que puerto se encuentran la estación con MAC 6, en la figura 2.10 se muestra este proceso de envío de trama a la estación C.

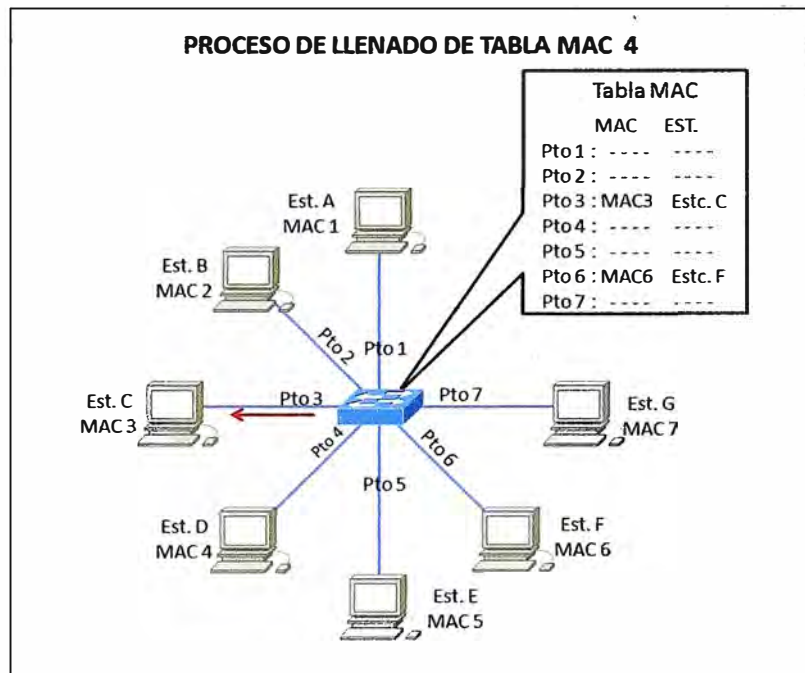


Figura 2.10 Proceso de llenada de tabla MAC 4

Los switches tienen diferentes formas de enviar una trama, los métodos de mayor uso son los siguientes:

- Método de almacenamiento y envío: Para este método el switch recibe la toda la trama entrante en uno de sus puertos y realiza la verificación del CRC, si en caso estuviera correcta y sin errores busca en su tabla de direccionamiento MAC la interfaz a la cual debe enviar la trama, en caso que el CRC tuviera un error lo descarta.
- Método de corte: Para este método al switch únicamente la basta con conocer la dirección MAC destino que tiene la trama, para buscar en la tabla de direccionamiento MAC la interfaz de salida, este método tiene menor latencia que el método de almacenamiento y envío, sin embargo no garantiza que la transmisión no tenga errores.

Algunos switches pueden trabajar con el método de corte configurado en todos sus puertos, sin embargo de llegar a ocurrir demasiados errores en la transmisión de la información, por encima de un umbral definido, puede cambiar automáticamente al método de almacenamiento y envío.

Una vez que los errores estén por debajo del umbral permitido, el método de envío configurado en el puerto puede cambiar automáticamente al método de corte.

2.3. Modelo TCP/IP

El modelo TCP/IP es la base sobre la cual se desarrolla actualmente el internet, debido a su sencillez y a su gran poder de aplicación se ha convertido en la actualidad en el modelo más usado en todo el mundo.

Una gran ventaja del modelo TCP/IP es que permite que redes de diferentes tecnologías físicas puedan comunicarse entre ellas sin problemas, debido a que estas tecnologías son solo una interface de acceso hacia una red siendo transparente para la pila de protocolos TCP/IP.

Por otro lado TCP/IP contempla que estas redes físicas puedan estar geográficamente distantes lo que es una ventaja adicional al momento de adoptar este modelo para la interconexión de redes.

A pesar que diferentes tipos de tecnologías de red física podrían trabajar sin problemas con el modelo TCP/IP ha sido Ethernet la tecnología física de acceso que ha tenido mayor aceptación y uso en redes LAN.

2.3.1. Protocolo de Internet (IP)

El protocolo de internet permite la comunicación entre estaciones de diferentes redes, ocultando su dirección física, creando en cierto modo una conexión virtual al momento de transmitir los datagramas de una estación a otra.

IP es un protocolo no orientado a conexión para el envío de paquetes que trabaja en base al mejor esfuerzo (best-effort), esto quiere decir que algunos paquetes enviados por IP pueden perderse, llegar en desorden o duplicados; IP asume que estos errores serán corregidos por los protocolos de las capas superiores.

• Direccionamiento IP

Las direcciones IP se representan mediante una secuencia de 32 bits o también de forma simplificada se representa mediante cuatro números decimales separados por puntos, por ejemplo el 201.230.120.209 es una dirección IP válida.

Toda dirección IP consta de dos partes:

$$IP\ address = \langle\ Dirección\ de\ red \rangle \langle\ Dirección\ de\ Host \rangle \quad (2.1)$$

Las direcciones IP son usadas por el protocolo IP para identificar una estación de modo único en una conexión de varias redes o de modo general en cualquier internet.

Cada estación capaz de enviar y recibir datagramas IP debe tener una dirección IP asignada, los datagramas son enviados a través de la conexión de red física a la que

están conectadas las estaciones, cada datagrama en su interior contiene una dirección de origen y una dirección de destino.

Para que el datagrama llegue a la dirección IP destino correcto debe ser traducida a la dirección física a la que está asociada.

• Clases de direcciones IP

Los primeros bits de de las direcciones IP indican cómo están separados tanto el número de red como el número de host dentro de los 32 bits de una dirección IP, esto en base a las clases de direcciones que se tienen establecidas, en la figura 2.11 se muestran las clases de direcciones IP.

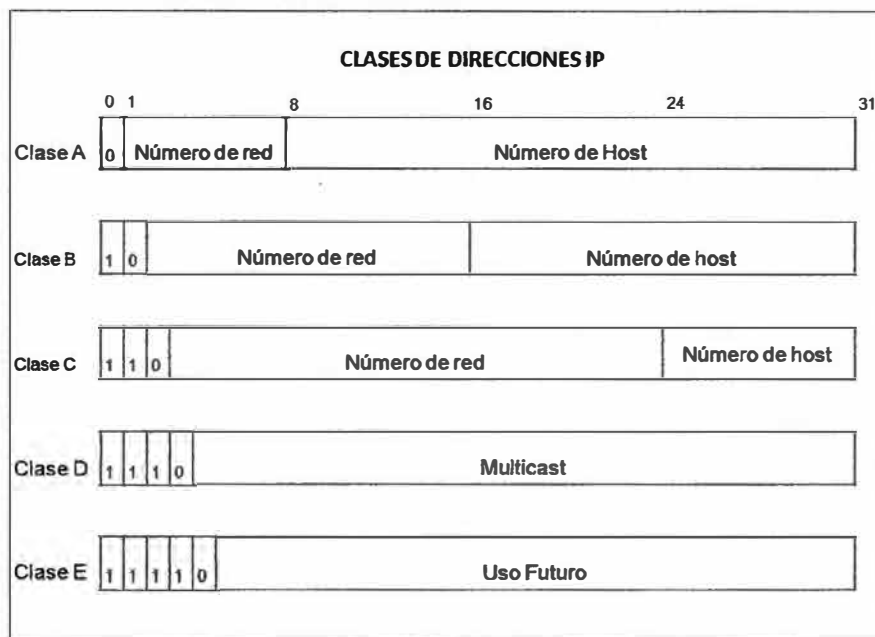


Figura 2.11 Clases de direcciones IP

Realizando los cálculos correspondientes obtenemos la tabla N° 2.1 en la cual se muestran los valores a considerar para cada una de las clases de direcciones IP.

TABLA N° 2.1 Clases de direcciones IP

Clase	Intervalo del primer octeto	Total de redes	Total de host por red	Mascara	Uso
A	1-126	126	16.7 millones	255.0.0.0	Clase estándar
B	128-191	16384	65534	255.255.0.0	Clase estándar
C	192-223	2 millones	254	255.255.255.0	Clase estándar
D	224-239	Sin definir	Sin definir	224.0.0.0	IP multidifusión
E	240-255	Sin definir	Sin definir	Sin definir	Experimental

• Subredes IP

Debido al rápido crecimiento de las redes en todo el mundo, el modo de direccionamiento en base a clases se hacía poco práctico y poco flexible. A fin de evitar estos inconvenientes se usa el concepto de subred IP, este concepto se aplica solo a nivel de la red local, toda la red continúa apareciendo con una dirección IP ante el resto de redes.

Para aplicar la técnica de subredes IP el número de host se divide en dos sub partes, una que tiene el término de número de subred y otro como número de host, ahora la red principal consta de varias subredes, el nuevo esquema es el siguiente:

$$IP\ address = \langle\ Número\ de\ red \rangle \langle\ Número\ de\ subred \rangle \langle\ Número\ de\ Host \rangle \quad (2.2)$$

La cantidad de bits elegidos para realizar el subneteo es de acuerdo a las necesidades que se quieran cubrir, por ejemplo si se requieren mayor cantidad de subredes entonces los bits designados para la parte de subred deben ser los suficientes para cubrir esta necesidad, por otro lado si se requiere una mayor cantidad de host para cada subred entonces los bits designados para la parte de host debe cubrir esta necesidad.

Por lo tanto cuantos más bits existan en el área de “Número de subred” entonces menor cantidad de “Número de host “resultará por cada subred y viceversa.

Existen dos tipos de subneteo; estático y de longitud variable siendo el subneteo de longitud variable es más flexible que el estático.

- Subneteo Estático

En el subneteo estático todas las subredes obtenidas desde una misma red usan la misma máscara, por un lado es simple de implementar y fácil de mantener, pero su uso desperdicia direcciones IP para redes pequeñas, por ejemplo una red de 50 host usando una máscara de subred 255.255.255.0 desperdicia más de 200 direcciones IP.

- Subneteo de longitud variable

En la práctica pueden existir redes con diferentes cantidades de host en cada una de ellas, por lo cual se ha definido el método de subneteo de longitud variable (VLSM), esto permite que dentro de la misma red se usen diferentes máscaras de subred haciendo más efectivo el uso de las direcciones IP al momento de realizar el subneteo.

Por ejemplo una subred pequeña con solo unos pocos hosts puede usar una máscara que se acomode a esa necesidad, una subred con varios hosts requiere una máscara de subred diferente, la habilidad de asignar mascarar de subred de acuerdo a las necesidades de cada subred ayuda a conservar las direcciones de red.

El subneteo de longitud variable divide la red para que cada subred contenga las direcciones suficientes para soportar el número requerido de host en cada caso.

Actualmente la gran mayoría de protocolos de enrutamiento trabajan sin problema con redes en las cuales se ha aplicado el VLSM.

• CIDR (Classless Interdomain Routing)

El objetivo inicial de CIDR era permitir que los IPS (proveedores de servicios de internet) puedan manejar bloques de direcciones IP de mayor o menor tamaño y no estar sujetos a una clase en particular, por ejemplo un IPS puede ofrecer a su cliente un bloque de direcciones IP publicas que pueden variar de 2 a 64 direcciones IP publicas según las necesidades de dicho cliente.

La idea básica de CIDR es olvidarse de las clases, un usuario tendrá control solo en el bloque de direcciones IP asignado, sin importar la clase que sea, este concepto ayuda a reducir de manera considerable el tamaño de las tablas de enrutamiento de los equipos routers, gracias a la sumarización de rutas que podría ejecutar.

2.3.2. Protocolo de datagrama de Usuario - UDP

UDP es un protocolo estándar descrito en el RFC 768 – User Datagram Protocol, este protocolo es usado por casi todas las aplicaciones TCP/IP que transmiten cantidades pequeñas de datos o que pueden darse el lujo de perder algo de datos durante una transmisión.

UDP es una interface de las aplicaciones a IP, no adiciona confiabilidad ni control de flujo o recuperación de errores a IP, simplemente funciona como un multiplexor/demultiplexor para el envío y recepción de datagramas, usa los puertos para direccionar los datagramas, en la figura 2.12 se muestra el modo de trabajo de UDP.

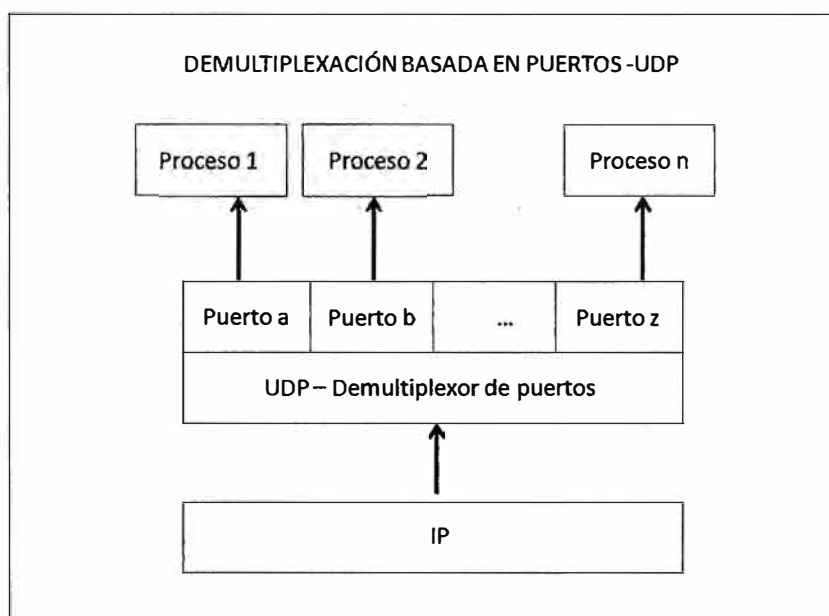


Figura 2.12 Demultiplexación basada en puertos UDP

UDP proporciona un mecanismo para que una aplicación envíe un datagrama a otra aplicación, la capa UDP puede ser considerada como muy simple y en consecuencia muy eficiente y rápida, pero esto requeriría que la aplicación deba asumir la responsabilidad de recuperar errores en la transmisión.

Las aplicaciones que envían datagramas a otros hosts necesitan una manera de identificar a que aplicación desean enviar los datos, esta especificación va mas allá de la dirección IP, ya que la dirección IP hace referencia a un sistema como un todo, para esta identificación UDP (y TCP) utiliza los números denominados puertos, que es un identificador de aplicación entendible por TCP/IP.

• Formato de datagrama UDP

Cada datagrama UDP es enviado dentro de un datagrama IP, aunque los datagramas IP pueden ser fragmentados durante la transmisión, estos fragmentos son reensamblados en el destino antes de ser enviados a la capa UDP.

Todas las implementaciones IP aceptan datagramas de 576 bytes, eso significa que, considerando el máximo tamaño de la cabecera IP de 60 bytes entonces un datagrama UDP tiene 516 bytes que es lo que comúnmente se encuentra en las implementaciones, en la figura 2.13 se muestra el formato del datagrama UDP.

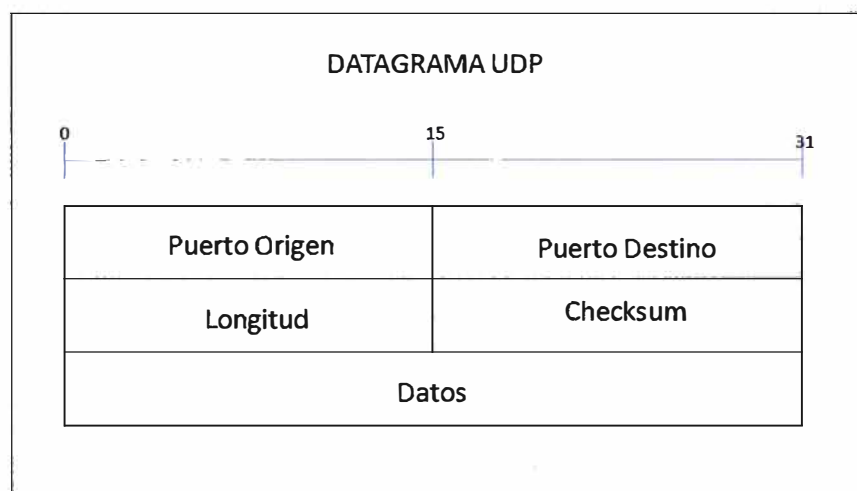


Figura 2.13 Datagrama UDP

- Puerto Origen: Indica el puerto del proceso que envía. Es el puerto al cual las respuestas están dirigidas, tiene 16 bits, es opcional en caso de no usar se completan con ceros.
- Puertos Destino: Indica el puerto del proceso destino en el host destino, consta también de 16 bits.
- Longitud: La longitud (en bytes) que se indica en este campo incluye la cabecera.
- Checksum: Este campo también es opcional, y es una suma de comprobación de 16 bits que abarca una pseudo-cabecera IP (con las IP origen y destino, el protocolo y la

longitud del paquete UDP), la cabecera UDP, los datos y 0's hasta completar un múltiplo de 16.

Algunas aplicaciones que usan UDP, se listan en la tabla N° 2.2

TABLA N° 2.2 Servicios que usan UDP

Servicios UDP	Puerto
Protocolo TFTP	69
Servicio DNS	53
Protocolo SNMP	161
Protocolo DHCP	68

Muy a menudo, las aplicaciones UDP no emplean mecanismos para garantizar la confiabilidad del envío de sus datagramas, por lo que si una aplicación requiere un alto grado de confiabilidad debe usar el protocolo TCP.

2.3.3. Protocolo de control de la transmisión - TCP

TCP brinda muchas más facilidades para las aplicaciones que UDP. Específicamente incluyen recuperación de errores, control de flujo y confiabilidad, TCP es un protocolo orientado a conexión, distinto a UDP que es un protocolo no orientado a conexión. Muchas de las aplicaciones de usuarios como Telnet y FTP, usan TCP.

El propósito de TCP es brindar un circuito lógico confiable entre un par de procesos, TCP no asume la confianza de los protocolos de capas inferiores (como IP), por lo tanto TCP debe garantizar confianza por sí mismo.

TCP se caracteriza por las siguientes facilidades que brinda a los protocolos lo usan:

- Transferencia de flujo de datos: Desde el punto de vista de la aplicación, TCP transfiere un flujo de bytes seguido a través de la red. La aplicación no se molesta en cortar el flujo en datagramas, esto lo hace TCP quien agrupa los bytes en segmentos TCP, los cuales son pasados a las capa IP para la transmisión hacia el destino, además TCP decide como segmentar la data, y puede transmitir los datos en su propia conveniencia.
- Confiabilidad: TCP asigna un número de secuencia para cada byte transmitido, y espera un acuse de recibo (ACK) de la capa TCP que recibirá. Si un ACK no es recibido dentro de un intervalo de tiempo, la data es retransmitida.
- El número de secuencia es usado para reordenar los segmentos cuando llegan en desorden y para eliminar segmentos duplicados.
- Control de Flujo: El receptor TCP al devolver un ACK al remitente también le indica la cantidad de números de bytes que puede recibir sin causar saturación y desborde en

sus memorias internas. Esto es enviado en el ACK en la forma del más alto número de secuencia que puede recibir sin problema.

- Multiplexación: Se logra a través del uso de los puertos, al igual que con UDP.
- Conexiones lógicas: La confiabilidad y el mecanismo de control de flujo requieren que TCP inicialice y mantenga cierta información de estado de cada flujo de datos. La combinación de este estado, incluidas los sockets, números de secuencia y tamaños de ventana, se le conoce como una conexión lógica.
- Full dúplex: TCP establece flujos de datos simultáneos en ambas direcciones.

Un protocolo de transmisión de manera simple se basa en el siguiente principio, el emisor transmite un paquete y espera recibir una notificación de recibo por parte del destino para poder enviar el siguiente paquete, si la notificación de recibo no es enviada dentro de un tiempo determinado, retransmite el paquete.

A pesar de que un protocolo así es confiable resulta poco práctico si se desea transmitir grandes cantidades de datos en poco tiempo.

• Cabecera del segmento TCP

En la figura 2.14 se muestra el formato de la cabecera TCP, asimismo se detallan cada una de sus partes.

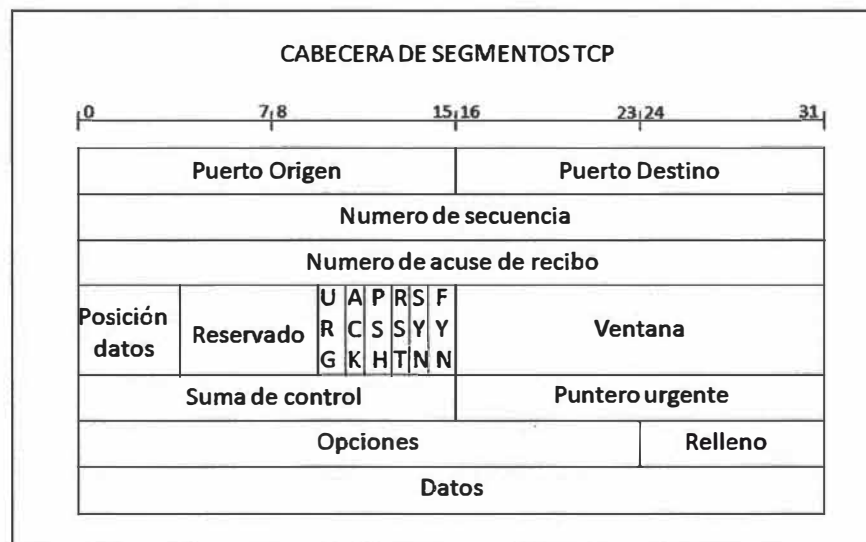


Figura 2.14 Cabecera de segmentos TCP

- Puerto origen: Consta de 16 bits indica el puerto usado por la aplicación origen, es usado por el receptor para responder durante la comunicación.
- Puerto destino: Consta de 16 bits indica el puerto usado por la aplicación destino.
- Número de secuencia: El número de secuencia del primer byte de datos en este segmento.

- Número de acuse de recibo: si el bit de ACK está configurado, este campo contiene el valor del siguiente número de secuencia que el receptor está esperando recibir.
- Reservado: Seis bits reservados para uso futuro, deben estar en cero.
- URG: Indica que el campo puntero urgente es importante en este segmento.
- ACK: Indica el campo de acuse de recibo (ACK)
- PSH: Función de PUSH (empuje)
- RST: Reseteo de la conexión.
- SYN: Sincroniza los números de secuencia.
- FYN: No más datos del transmisor.
- Ventana: Indica el número de bytes de datos que está dispuesto a aceptar.
- Suma de control (checksum): Es la suma de comprobación de 16 bits que abarca una pseudo-cabecera IP (con las IP origen y destino, el protocolo y la longitud del paquete TCP), la cabecera TCP, los datos y 0's hasta completar un múltiplo de 16.

2.4. Tecnología voz sobre IP – VoIP

2.4.1. Funcionamiento de la voz sobre IP

En primer lugar se debe tener en cuenta que la voz tiene que ser digitalizada. Como segundo proceso viene la supresión de las señales no deseadas y la compresión de las señales de voz, a su vez este proceso se divide en dos subprocesos.

En el primero el sistema examina las señales recientemente digitalizadas y determina si contienen señales de voz o ruidos y descarta algún paquete que no contenga audio, por otro lado se usan algoritmos complejos para reducir la cantidad de información que es enviada de un teléfono a otro, estos códigos son capaces de suprimir el ruido y comprimir el tráfico de voz, algunos ejemplos son G.723, G.728, G.729.

Luego de la digitalización y la compresión, la voz debe ser paquetizada para ser transmitidos a través de la red IP.

En redes IP, un porcentaje de los paquetes enviados pueden perderse o retrasarse especialmente en periodos de congestión, además algunos paquetes pueden ser descartados durante la transmisión por los errores que pueden presentar, estas pérdidas, los retrasos y daños de los paquetes afectan considerablemente la calidad de la voz.

Dado lo sensible de la voz para un sistema de telefonía, el sistema de VoIP no puede esperar por retransmisiones, por ese motivo se emplean mecanismos más sofisticados de detección de errores, además sistemas de corrección son usados para crear sonidos y llenar los vacíos para los paquetes que no llegan al destino, este proceso almacena una porción de la voz entrante del emisor y luego usando un algoritmo complejo aproxima el contenido de los paquetes perdidos, de esta manera el sonido escuchado por el receptor

no es exactamente el sonido transmitido sino que porciones de ella se van creando por el sistema para mejorar el sonido entregado al receptor.

Un sistema de VoIP está conformado por un conjunto de protocolos que permiten su funcionamiento, para VoIP los protocolos más importantes se dividen en: señalización, enrutamiento y transporte.

Los protocolos de señalización (H.323 y Session Initiation Protocol [SIP]), establece el circuito virtual sobre la red por donde pasara el flujo de datos, la señalización es independiente al flujo de datos, asimismo determina el tipo de medio usado en una llamada.

Una vez que la ruta del flujo de datos (conversación) ha sido establecida empieza el uso de los protocolos que enrutarán la conversación (UDP y TCP) y los protocolos de transporte (Real-Time transport protocol RTP).

2.4.2. Protocolo H.323

H.323 es una especificación del sector de Telecomunicaciones de la Unión Internacional de Telecomunicaciones (ITU-T) para la transmisión de audio, video y datos a través de una red IP, incluido internet.

H.323 permite también la interoperabilidad entre diferentes marcas, el estándar H.323 direcciona señalización y control de llamadas, transporte y control multimedia además del control de ancho de banda para comunicaciones punto a punto o multipunto.

En la tabla N° 2.3 se muestra los componentes y protocolos que se usan en H.323.

TABLA N° 2.3 Componentes y protocolos en H.323

Característica	Protocolo
Señalización de llamada	H.225
Control de medio	H.245
Audio Codecs	G.711, G.722, G.723, G.728, G.729
Video Codecs	H.261, H.263
Compartición de Data	T.120
Medios de transporte	RTP/RTCP

En la figura 2.15 se muestran los elementos de una red H.323, los terminales permiten comunicaciones punto a punto y multipunto para audio, y opcionalmente video y datos. Los gateways son los elementos que conectan una zona H.323 con la red de telefonía pública (PSTN), Gatekeepers brindan control de admisión y servicio de traducción de direcciones para terminales y gateways. Los MCU son dispositivos que permiten a dos o más terminales o gateways comunicaciones de audio y/o sesiones de video

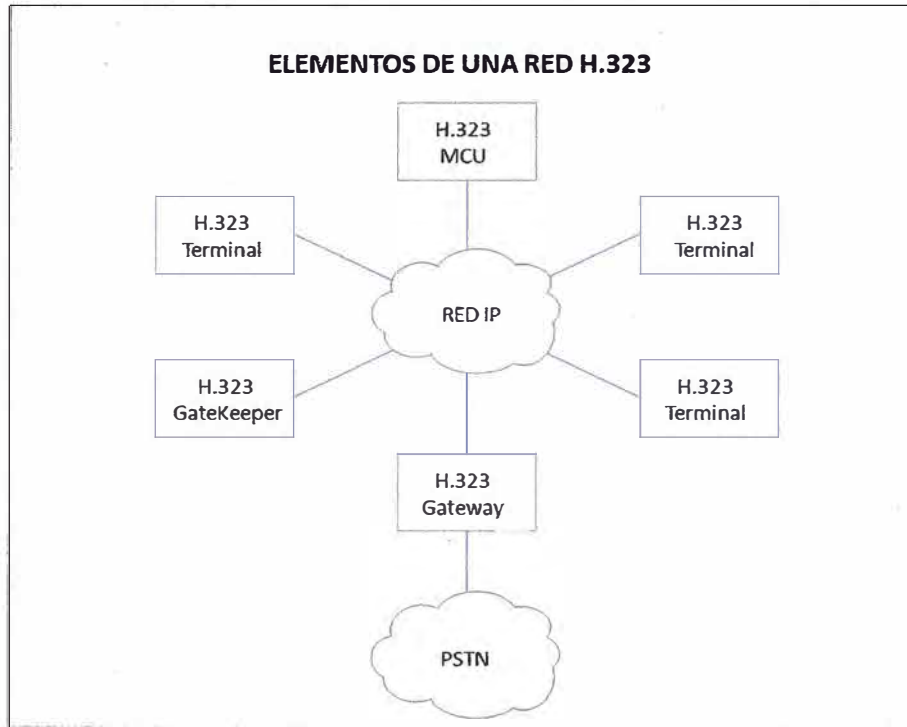


Figura 2.15 Terminación de sesión TCP

• **Terminal**

Los terminales H.323 deben tener una unidad de sistema de control, medio de transmisión, códec de audio y una interface para una red basada en paquetes (como TCP/IP), opcionalmente requiere un códec de video y aplicaciones de datos para usuarios, en la figura 2.16 se muestra la composición de un elemento H.323

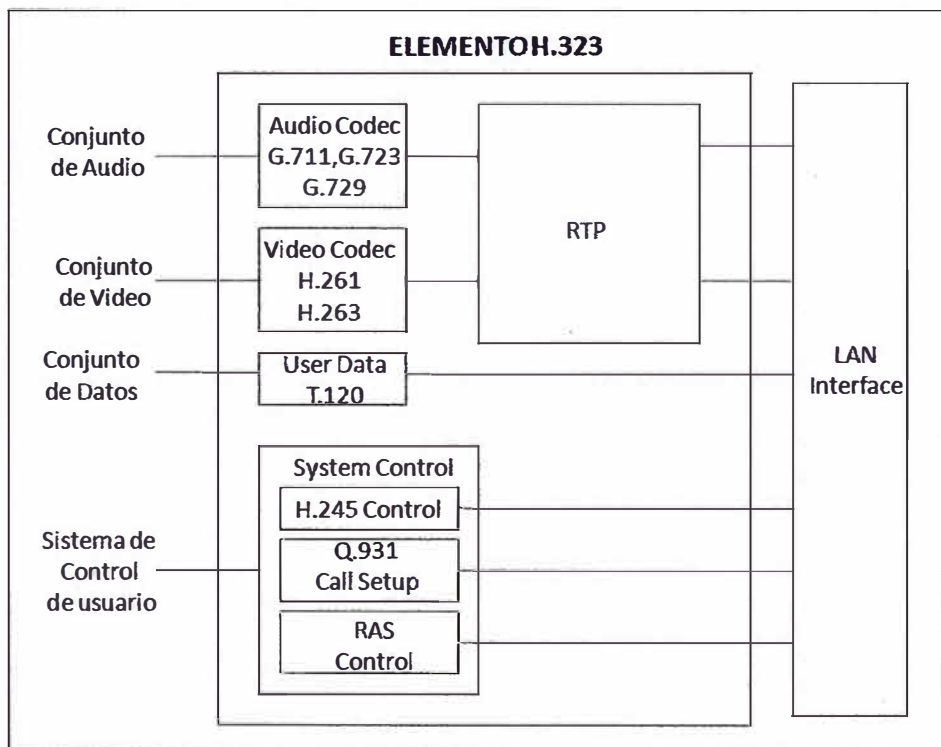


Figura 2.16 Elemento H.323

Las siguientes funciones y capacidades se encuentran dentro de un terminal H.323:

- Unidad de sistema de control: Proporciona H.225 y control de llamada con H.245, intercambio de capacidades, mensajería, y señalización de comandos para una correcta operación de los terminales.
- Medio de transporte: Formatos transmitidos de audio, video, datos, flujos de control, y mensajes de la interface de red.
- Codec de audio: Codifica la señal del equipo de audio para la transmisión y decodifica el código de audio entrante, funciones requeridas incluyen codificar y decodificar audios en G.711 y transmitir y recibir formatos en Ley-a y en Ley- μ , opcionalmente G.722, G.723.1, G.728 y G.729 pueden ser soportados para la codificación y decodificación .
- Interfaz de red: interfaz basada en paquetes con la capacidad de sesiones punto a punto TCP y sesiones UDP para servicios unicast y multicast.
- Codec de video: Es opcional, pero si es brindando debe ser capaz de decodificar y codificar video de acuerdo a los protocolos H.261 y H.263.
- Canal de datos: Soporta aplicaciones como acceso a base de datos, transferencia de archivos y conferencias audiográficas (la capacidad de modificar una imagen común por múltiples usuarios a la vez), Tal como se especifica en la Recomendación T.120

• Gateway

Un Gateway H.323 refleja las características de un terminal en una red de circuitos conmutados (SCN) y un terminal H.323. Traduce entre formatos de audio, video y transmisión de datos, asimismo sistemas de comunicación y protocolos. Esto incluye establecimiento de la llamada y finalización, tanto en la red IP como en la SCN.

Los Gateway no son necesarios a menos que se requiera una interconexión con la SCN. Por lo tanto terminales H.323 se comunican directamente con otros a través de una red IP sin necesidad de un Gateway, en la figura 2.17 se muestra la composición del gateway.

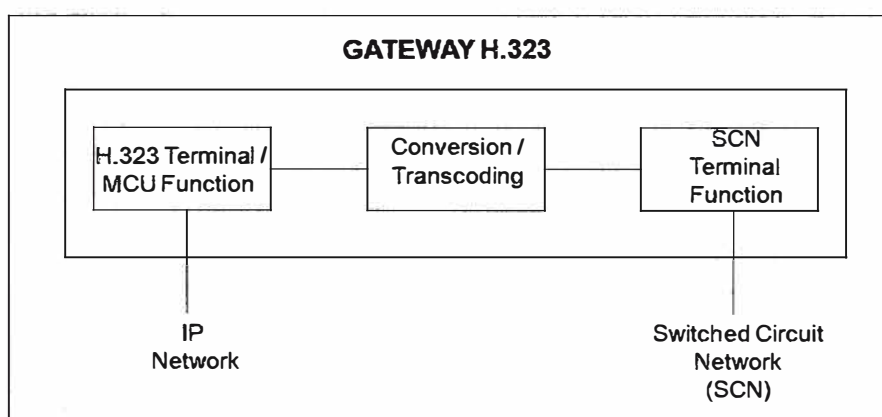


Figura 2.17 Gateway H.323

• Gatekeeper

El gatekeeper puede ser considerado como el cerebro de una red H.323. Es el punto focal para todas las llamadas dentro de una red H.323 dado que brindan importantes servicios como direccionamiento, autorización y autenticación de los terminales y gateways, control del ancho de banda, contabilización, facturación y cobro. Asimismo los gatekeepers pueden proporcionar el servicio de enrutamiento de las llamadas.

• Unidades de control Multipunto (MCU)

MCU brinda soporte para conferencias de tres o más terminales H.323. Todos los terminales que participan en la conferencia establecen una conexión con el MCU. Los MCU controlan los recursos de conferencia, negocia con los terminales con el propósito de determinar los códec de audio o video a usarse, y puede manejar el flujo a través del medio.

2.4.3. Conjunto de protocolos H.323

El protocolo H.323 está basado en varios protocolos como se muestra en la figura 2.18, la familia de protocolos soporta admisión de llamadas, configuración, estado, culminación, transmisiones multimedia y mensajes en los sistemas H.323.

En la figura 2.18 se muestra el conjunto de protocolos H.323.

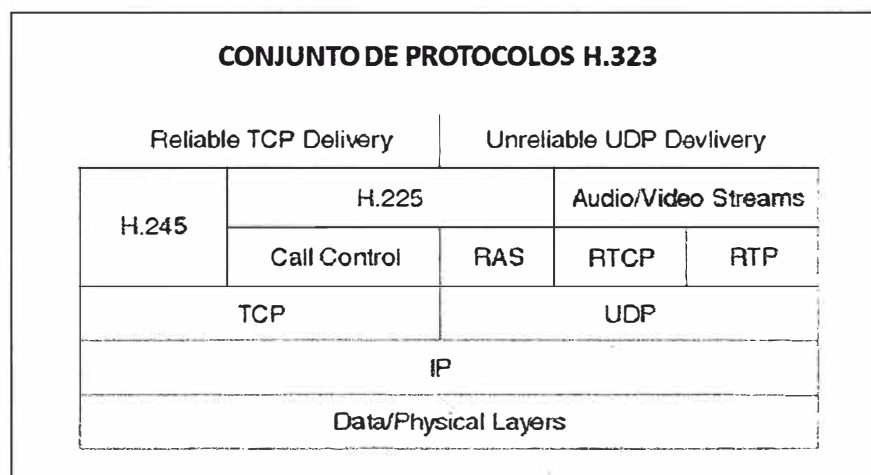


Figura 2.18 Conjunto de protocolos H.323

Estos protocolos son soportados tanto para TCP como UDP, sin embargo en la actualidad es UDP el protocolo que está siendo usado con mayor frecuencia para soportar este conjunto de protocolos.

El conjunto de protocolos H.323 esta dividido en 3 principales áreas de control:

- Señalización registro, admisión y estatus (RAS) – brinda control de pre-llamada en redes H.323 gobernadas por un gatekeeper

- Señalización de control de llamada – usado para conectar, mantener y desconectar llamadas entre puntos finales.
- Control de medio y transporte - Brinda un canal confiable H.245 que transporta mensajes de control de medio, el transporte se produce en un flujo no confiable del protocolo UDP.

- **Protocolo de tiempo-real (RTP) (real-time transport protocol)**

El protocolo RTP tiene como objetivo asegurar una QoS para servicios en tiempo real. Incluye la identificación del payload, la numeración secuencial, la medición de tiempo y el reporte de la calidad (protocolo RTCP).

Este protocolo RTP es de transporte (capa 4) y trabaja sobre UDP de forma que posee un checksum para detección de error y la posibilidad de multiplexación de puertos UDP. Las sesiones de protocolo RTP pueden ser multiplexadas. Para ello se recurre a un doble direccionamiento mediante las direcciones IP y el número de puerto en UDP.

El RTP funciona en conjunto con RSVP (capa 3) para la reservación de ancho de banda y asegurar de esta forma la calidad del servicio QoS del tipo Garantizada. La QoS del tipo Diferenciada se logra mediante la priorización de tráfico.

- **Protocolo de control RTCP (real-time control protocol)**

Este protocolo permite completar a RTP facilitando la comunicación entre extremos para intercambiar datos y monitorear de esta forma la calidad de servicio y obtener información acerca de los participantes en la sesión. RTCP se fundamenta en la transmisión periódica de paquetes de control a todos los participantes en la sesión usando el mismo mecanismo RTP de distribución de paquetes de datos. El protocolo UDP dispone de distintos puertos como mecanismo de identificación de protocolos. La función primordial de RTCP es la de proveer una realimentación de la calidad de servicio; se relaciona con el control de congestión y flujo de datos.

- **CRTP**

Para reducir el ancho de banda consumido por los códec, por ejemplo G.729, se usa cRTP, el cual permite comprimir una cabecera a fin de que el ancho de banda usado sea menor.

Como se aprecia en la figura 2.19 la cabecera de paquete IP, UDP y RTP ha sido reducida de un valor de 40 Bytes a solo 2 o 4 Bytes.

Con un paquete reducido de esa manera se procede a enviar la información a través de la tecnología de capa 2 usada, en nuestro caso será Ethernet.

En la figura 2.19 se muestra todo el proceso de compresión cRTP.

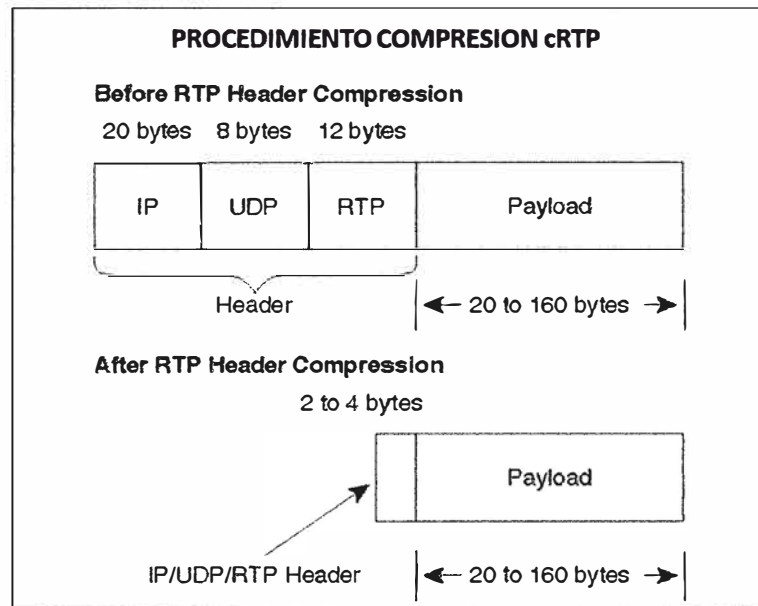


Figura 2.19 Procedimiento compresión cRTP

2.5. Tecnología de conexión punto a punto

Como se indicó anteriormente la comunicación de segmentos de red diferentes es llevada a cabo por los equipos de enrutamiento de capa 3, por ejemplo los routers, sin embargo a nivel de la capa física y de la capa de enlace de datos del modelo OSI se requiere el uso de tecnologías que permitan la conexión a redes que físicamente se encuentran fuera de nuestra red LAN ya sea a poca o a mediana distancia.

Existen diferentes maneras de lograr la conexión entre de dos sitios, a continuación mencionaremos algunas de ellas.

2.5.1. Conexión de dos puntos por intermedio de fibra óptica

Fibra oscura es la denominación popular que se atribuye a los circuitos de fibra óptica que han sido desplegados por algún operador de telecomunicaciones pero no están siendo utilizados. La conectividad por la fibra se comercializa en bruto, de manera que es el propio cliente quien aplica la tecnología de transmisión que más se adecua a sus necesidades, mejorando así el rendimiento obtenido puesto que se evitan conversiones innecesarias de protocolos.

Este tipo de conexión resulta ser muy útil debido a que la conexión entre los puntos se hace prácticamente sin intervención de ningún equipo intermedio, este servicio implica un gasto por el arrendamiento mensual del uso de la fibra óptica oscura.

En la figura 2.20 se muestra el detalle de conexión de dos puntos a través de una fibra óptica oscura.

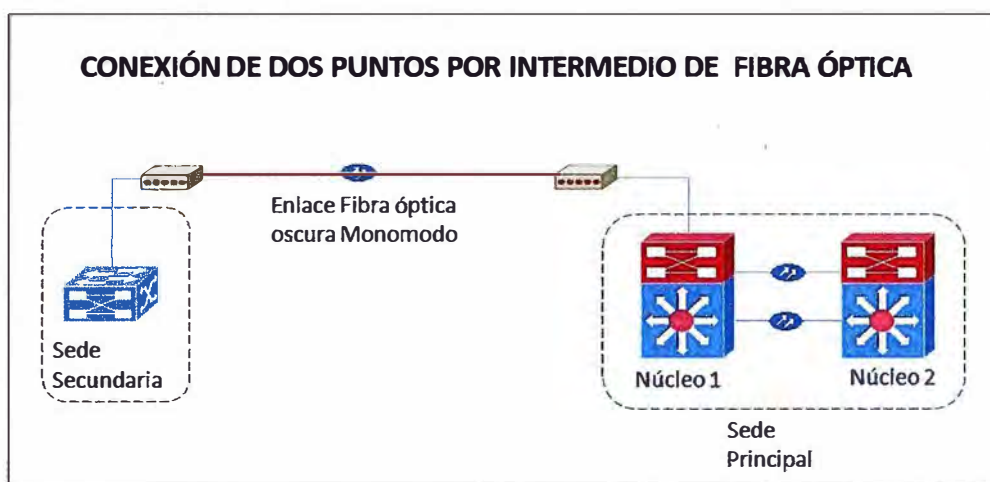


Figura 2.20 Conexión de dos puntos por intermedio de f.o.

2.5.2. Conexión de dos puntos por intermedio de un radio enlace

El uso de la solución de un radio enlace para interconectar por sedes distantes, ha ido en aumento los últimos años, debido a su practicidad de la instalación, el poco mantenimiento que requieren, el costo que es menor en muchos casos que alquilar un enlace de fibra óptica.

La consideración más importante durante el dimensionamiento de esta solución es que los puntos donde estarán instalados los radio enlaces debe tener línea de vista entre ellos, esta tecnología usa frecuencias de portadora por encima de 1GHz, por tal motivo se encuentran en el grupo de las súper altas frecuencias (SHF).

La mayoría de frecuencia de los enlaces de radio requieren de licencias para su uso, sin embargo existen bandas libres que pueden ser usadas para la instalación de un radio enlace, por ejemplo la banda de los 5 GHz; debido a esto se ha incrementado el uso de los radios enlaces punto a punto cuando la solución cableada no es factible, en la figura 2.21 se muestra el detalle de conexión por intermedio de un radio enlace.

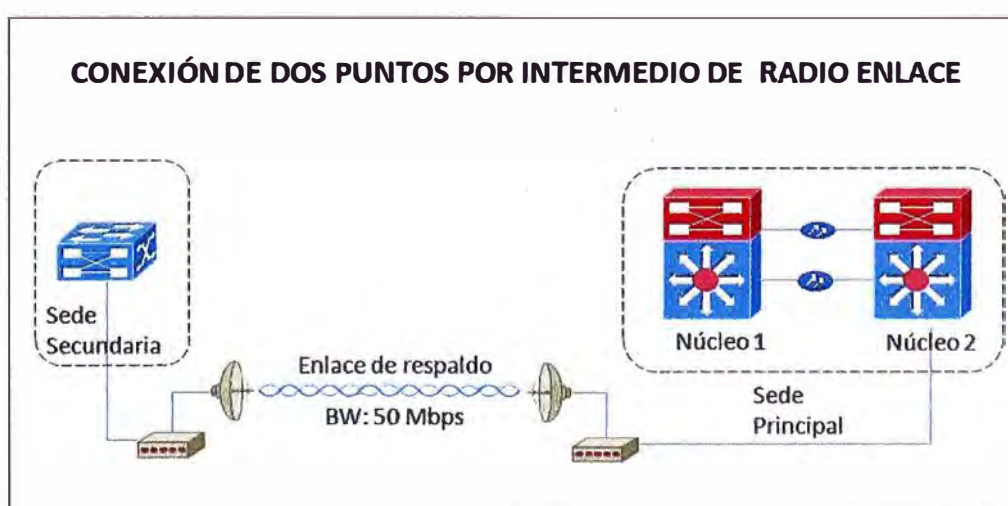


Figura 2.21 Conexión de dos puntos por intermedio de radioenlace

2.5.3. Conexión de dos puntos por intermedio de la red de un tercero

La conexión de dos puntos por intermedio de la red de un proveedor externo generalmente usa una red de transporte desplegada a lo largo de una gran extensión geográfica, para fines de este informe estas tecnologías serán transparentes; se opta por este tipo de conexión cuando las sedes a conectar están físicamente distantes y el uso de una fibra oscura no es factible por lo alto del costo, en la figura 2.22 se muestra el modo de conexión entre dos sedes cuando se usa la red de transporte de un proveedor.

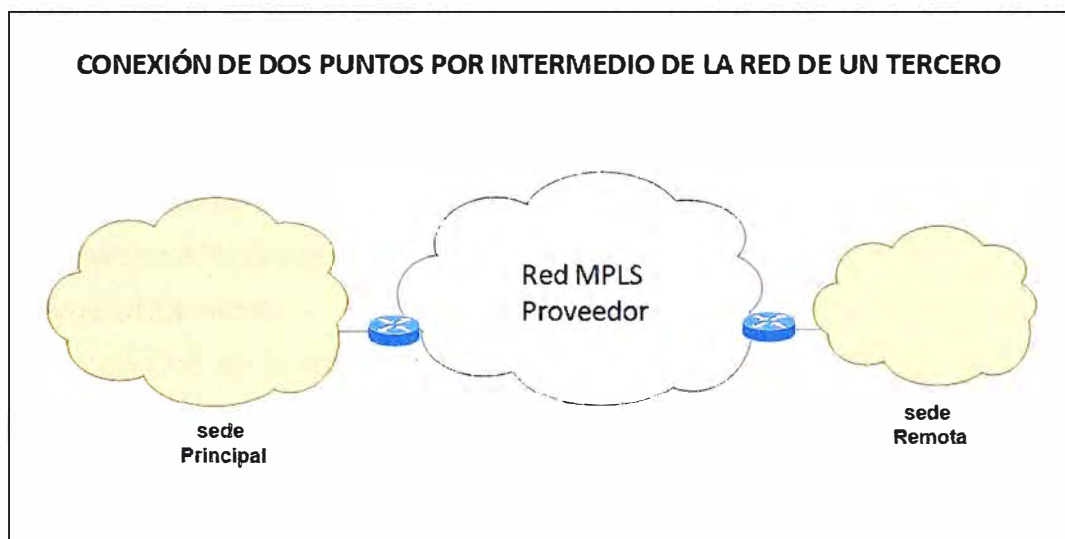


Figura 2.22 Conexión de dos puntos por intermedio de la red de un tercero

2.6. Calidad de servicio

La calidad de servicio busca asegurar una tasa de datos en la red (ancho de banda), un retardo y una variación de retardo (jitter) acotados a valores contratados con el cliente. Para disponer de una calidad de servicio aceptable en redes soportadas en protocolo IP se han diseñado herramientas a medida como son los protocolos de tiempo-real RTP y de reservación RSVP.

Los servicios tradicionales de la red Internet disponen de una calidad denominada "best effort"; es decir que la red ofrece el mejor esfuerzo posible para satisfacer los retardos mínimos; lo cual no es mucho pero es suficiente para servicios que no requieren tiempo-real como el web sin embargo para servicios del tipo "real-time" (voz y vídeo) se requiere una latencia mínima.

Se denomina latencia a la suma de los retardos en la red. Los retardos están constituidos por el retardo de propagación y el de transmisión (dependiente del tamaño del paquete), el retardo por el procesamiento "store-and-forward" (debido a que los switch o router emiten el paquete luego de haber sido recibido completamente en una memoria buffer) y el retardo de procesamiento (necesario para reconocimiento de encabezado, errores, direcciones, etc.).

2.6.1. Tipos de calidad de servicio

Los servicios de datos y multimedia tienen distintos requerimientos de calidad con respecto a latencia y jitter. Para satisfacer los requerimientos de calidad se acude al manejo de las colas de paquetes, la reservación de ancho de banda y la gestión del tráfico. Para obtener estos objetivos en diversos ámbitos se han definido variantes de servicios.

A continuación indicamos las siguientes variantes de servicios:

- **CoS (Class of Service)**

CoS se logra mediante 3 bits que se ingresan en un campo adicional de 4 Bytes (etiqueta denominada Tag o Label) dentro del protocolo MAC. Estos 3 bits permiten definir prioridades desde 0 (máxima) a 7 (mínima) y ajustar un umbral en el buffer de entrada y salida del switch LAN para la descarga de paquetes.

- **ToS (Type of Service)**

Es sinónimo de CoS en la capa 3. Sobre el protocolo IP se define el ToS con 3 bits (del segundo byte del encabezado IP) para asignar prioridades. Se denomina señal de precedencia.

- **QoS (Quality of Service)**

En redes IP se define la tasa de acceso contratada CAR (Committed Access Rate) en forma similar al CIR de Frame Relay y ATM. La calidad QoS se ve garantizada mediante protocolos de reservación RSVP y protocolos de tiempo real RTP.

Clasificación de la QoS:

- **Guaranteed** - El servicio garantizado es utilizado para requerir un retardo máximo extremo-a-extremo. Al usuario se le reserva un ancho de banda dentro de la red para su uso exclusivo aún en momentos de congestión. Se lo conoce como Hard QoS.
- **Differentiated** - El servicio diferenciado utiliza la capacidad de particionar el tráfico en la red con múltiples prioridades o ToS (Type of Service). Se dispone de 3 bits de precedencia para diferenciar las aplicaciones sensibles a la congestión (se brindan mediante el encabezado del protocolo IPv4). Es por lo tanto un Soft QoS. La primera línea de defensa frente a la congestión es el uso de buffer de datos; lo cual implica el armado de una cola de espera y el retardo correspondiente dependiendo de la prioridad asignada en dicha cola.
- **Best-effort**. - Este es un servicio por default que no tiene en cuenta las modificaciones por la QoS. Se trata de una memoria buffer del tipo FIFO, trabaja sobre redes LAN y redes corporativas. Esta norma no tiene previsto garantizar la calidad de servicio QoS.

2.6.2. Formación de anillos

Se trata de configurar la red de switches con enlaces en loop para incrementar la redundancia. Los loops están prohibidos en Ethernet pero mediante el protocolo STP se puede configurar la red en forma automática para detectar los loops e interrumpirlos hasta que una falla los habilite como necesarios. Las posibles configuraciones son:

- El STP se puede habilitar para cada VLAN en particular.
- A los puertos se les asigna una prioridad y un costo para que STP determine el mejor camino.
- Se puede determinar el estado de un puerto (bloqueado, deshabilitado, forwarding, etc). Desde bloqueo a forward se pasa por listening (escuchar) y learning (aprender).
- PortFast es una función que habilita a pasar desde el bloqueo a forward sin pasar por los estados intermedios.
- UplinkFast permite una rápida convergencia para cambios con enlaces redundantes. Otra variante es BackboneFast.

Los puertos que utilizan la función STP se encuentra en algunos de los siguientes estados: bloqueado (no participa de la transmisión); listening (es un estado transitorio luego del bloqueo y hacia el forwarding), learning (es otro estado transitorio antes de pasar al forwarding); forwarding (transmite las tramas en forma efectiva) y deshabilitado (se trata del estado no-operacional).

Este protocolo permite identificar los loop y mantener activa solo un enlace del switch. Por otro lado, utiliza un algoritmo que permite identificar el mejor camino libre de loops en la red de switch. Para lograr este objetivo, se asigna a cada puerto un identificador consistente en la dirección MAC y una prioridad. La selección del puerto se puede asignar en términos de prioridad (valor entre 0 y 63; por default es 32) y costo (0 a 65535).

El STP consiste en un intercambio de mensajes de configuración en forma periódica (entre 1 y 4 seg.). Cuando se detecta un cambio en la configuración de la red (por falla o cambio de costo de los puertos) se recalcula la distancia (sumatoria de costos) para asignar una nueva puerta. Las decisiones se toman en el propio switch. En condiciones normales se selecciona un switch para que trabaje como switch raíz para determinar una topología de red estable (es el centro lógico de la topología en Tree). Por default el switch que posee la dirección MAC más baja es el seleccionado como raíz.

2.6.3. Reservación de ancho de banda (RSVP)

Los servicios del tipo "best effort" no prevén una calidad de servicio. Esto tiene como consecuencia una latencia variable y jitter sobre la información del tipo tiempo-real (audio

o vídeo). RSVP permite la reservación de ancho de banda para asegurar una QoS. El protocolo RSVP trabaja en conjunto con el protocolo de transporte RTP para servicios de voz y vídeo en tiempo-real. El RSVP está disponible en RFC-2205.

Existen dos formas de reservación del ancho de banda: estática y dinámica. La reservación estática permite asignar un porcentaje fijo del canal de comunicación a cada tipo de protocolo (por ejemplo, 10% a HTTP, 15% a FTP, 3% a Telnet, etc.). El protocolo RSVP permite reservar el ancho de banda en forma dinámica para asegurar una calidad de servicio QoS en las redes IP.

El protocolo RSVP se define para los servicios integrados en Internet. Es utilizado por el host para solicitar una QoS al router para una aplicación particular y es usado por el router para establecer un ancho de banda con todos los nodos intermedios del trayecto.

2.7. Seguridad de la información

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que protejan la información manteniendo la confidencialidad, la disponibilidad e integridad de la misma.

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología, si la información está centralizada puede tener un alto valor. Puede ser divulgada, mal utilizada, ser robada, borrada o sabotada. Esto afecta su disponibilidad y la pone en riesgo.

Las tres características fundamentales de la seguridad de la información son las siguientes:

- Confidencialidad

Es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados, la confidencialidad es el acceso a la información únicamente por personas que cuenten con la debida autorización.

- Integridad

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. La integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad.

- Disponibilidad

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. A groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.

La disponibilidad además de ser importante en el proceso de seguridad de la información, es además variada en el sentido de que existen varios mecanismos para cumplir con los niveles de servicio que se requiera. La gama de posibilidades dependerá de lo que queremos proteger y el nivel de servicio que se quiera proporcionar.

2.7.1 Seguridad perimetral

El Firewall es parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los firewall pueden ser implementados en hardware o software, o una combinación de ambos. Los firewall se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del firewall que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar al firewall a una tercera red, llamada "zona desmilitarizada" o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Tipos de firewall:

- Firewall de filtrado de paquetes: Típicamente es un router con la capacidad de filtrar paquetes, actúa en la capa 3 y en la capa 4 del modelo OSI.
- Firewall de estado: Monitorea el estado de las conexiones, si la conexión esta iniciada, transfiriendo datos o terminada, por su versatilidad es la tecnología de firewall que se emplea con mayor frecuencia en las redes corporativas.
- Proxy firewall: Actúa como relé entre dos redes mediante la intervención y la realización de una evaluación completa del contenido en los paquetes intercambiados. Por lo tanto,

el proxy actúa como intermediario entre los ordenadores de la red interna y la red externa, y es el que recibe los ataques. Este tipo de firewall es muy efectivo y si se ejecuta correctamente asegura una buena protección de la red. Por otra parte, el análisis detallado de los datos de la aplicación requiere una gran capacidad de procesamiento, lo que a menudo implica la ralentización de las comunicaciones, ya que cada paquete debe analizarse minuciosamente.

2.7.2. Seguridad dentro de la LAN

De la misma manera como se toman recaudos para asegurar una red de ataques externos, se deben considerar procedimientos para asegurar una red desde el interior de la misma, ya que las posibilidades de sufrir un ataque son tan o más altas desde el interior de la red que desde afuera.

El aseguramiento de la LAN debe mitigar ataques dentro de la infraestructura de la capa dos. Estos ataques incluyen suplantación de MAC address, Manipulación de STP, desborde de tablas de direcciones MAC, tormentas LAN etc.

- Suplantación de MAC address: Ocurre cuando un atacante altera la dirección MAC de su host para hacerlo coincidir con una MAC address conocida dentro de la red. El host atacante entonces envía una trama a través de la red con la nueva MAC address configurada, el switch almacena la nueva información y asocia la mac address del host objetivo al puerto de origen donde se encuentra el atacante.

De esta manera para las comunicaciones siguientes toda la información no llegaría al equipo verdadero si no que llegaría al equipo del atacante.

- Manipulación de STP: El host atacante mediante el envío de mensajes BPDU busca modificar la topología de tal manera que le permita a convertirse en el root brige (switch raíz).

- Desborde de tablas de direcciones MAC: Ocurre cuando el atacante envía múltiples tramas con direcciones origen falsa con la finalidad de saturar las tablas MAC de los switches, una vez que se logra esto el switch se comportara como un HUB y enviará las tramas siguientes a través de todos los puertos del switch, de esta manera un atacante podrá ver todo tipo de información.

- Tormentas LAN: Ocurren cuando mensajes de broadcast son enviados a través de la red LAN de manera continua, esto incrementa el procesamiento de los procesadores en el switches hasta en un 100% en poco tiempo y degrada el rendimiento de la red.

La forma de mitigar este tipo de eventos es la configuración de un control de tormenta, donde básicamente el switch contabiliza la cantidad de paquetes que pasan a través de sus puertos y determinan de qué tipo de tráfico es (unicast, multicast o broadcast),

cuando este tráfico supere un cierto umbral para un puerto en particular se procede con el bloqueo del puerto por un lapso de tiempo.

Con la finalidad de mitigar los potenciales riesgos de una red LAN se debe considerar el configurar los puertos de acceso de los switches en la LAN con seguridad de puerto, esto permitirá configurar una dirección MAC de forma estática o indicar la cantidad de direcciones MAC que se pueden esperar como máximo a través de un puerto en particular, indicando en caso ocurra un exceso de MAC alguna acción a modo de protección, (por lo general deshabilitar el puerto).

Por otro lado se deben tener habilitados solo los puertos de los switches que están en funcionamiento, por lo general siempre quedan puertos libres en la capa de acceso que se recomiendan dejar en estado apagado a fin de evitar que una tercera persona tenga un acceso no permitido a la red.

2.7.3. Tecnología de prevención de ataques

Sistema de prevención de intrusos (IPS) - Un Sistema de Prevención de Intrusos (IPS) es un dispositivo que ejerce el control de acceso en una red informática para proteger una red LAN de ataques y abusos.

Los IPS fueron inventados para resolver ambigüedades en el monitoreo pasivo de redes de computadoras, al situar sistemas de detecciones en la vía del tráfico. Los IPS presentan una mejora importante sobre las tecnologías de firewall tradicionales, al tomar decisiones de control de acceso basados en los contenidos del tráfico, en lugar de direcciones IP o puertos.

También es importante destacar que los IPS pueden actuar al nivel de equipo terminal de usuario, para combatir actividades potencialmente maliciosas.

Un Sistema de Prevención de Intrusos establece políticas de seguridad para proteger el equipo o la red de un ataque; se podría decir entonces que un IPS protege al equipo proactivamente, los IPS se categorizan en la forma que detectan el tráfico malicioso:

- Detección Basada en Firmas: Una firma tiene la capacidad de reconocer una determinada cadena de bytes en cierto contexto, y entonces lanza una alerta. Por ejemplo, los ataques contra los servidores web generalmente toman la forma de URLs. Por lo tanto se puede buscar utilizando un cierto patrón de cadenas que pueda identificar ataques al servidor Web. Sin embargo, como este tipo de detección funciona parecido a un Antivirus, el Administrador debe verificar que las firmas estén constantemente actualizadas.
- Detección Basada en Políticas: En este tipo de detección, el IPS requiere que se declaren muy específicamente las políticas de seguridad. Por ejemplo, determinar que

hosts pueden tener comunicación con determinadas redes. El IPS reconoce el tráfico fuera del perfil permitido y lo descarta.

- Detección Basada en Anomalías; Este tipo de detección tiende a generar muchos falsos positivos, ya que es sumamente difícil determinar y medir una condición 'normal'. En este tipo de detección tenemos dos opciones:
 - ✓ Detección Estadística de Anormalidades: El IPS analiza el tráfico de red por un determinado periodo de tiempo y crea una línea base de comparación. Cuando el tráfico varía demasiado con respecto a la línea base de comportamiento, se genera una alarma.
 - ✓ Detección No Estadística de Anormalidades: En este tipo de detección, es el administrador quien define el patrón 'normal' de tráfico. Sin embargo, debido a que con este enfoque no se realiza un análisis dinámico y real del uso de la red, es susceptible a generar muchos falsos positivos.
- Detección Honey Pot (Jarra de Miel): Aquí se utiliza un 'distractor'. Se asigna como Honey Pot un dispositivo que pueda lucir como atractivo para los atacantes. Los atacantes utilizan sus recursos para tratar de ganar acceso en el sistema y dejan intactos los verdaderos sistemas. Mediante esto, se puede monitorizar los métodos utilizados por el atacante e incluso identificarlo, y de esa forma implementar políticas de seguridad acordes en nuestros sistemas de uso real.

CAPÍTULO III DETERMINACIÓN DE NECESIDAD

3.1. Servicios a Prestar

La empresa objeto de este estudio se dedica a la elaboración y venta de productos de belleza y cuenta con varias oficinas en la ciudad de Lima. En la tabla N° 3.1 se muestran los servicios de datos y voz que brinda su red de telecomunicaciones a los usuarios.

TABLA N° 3.1 Servicios que brinda la red

Servicios de datos	Servicio de voz
<ul style="list-style-type: none">• Navegación a internet• Acceso a correo corporativo• Acceso a correo externo• Transferencia de archivos• Uso de la intranet corporativa• Publicación de servicios web	<ul style="list-style-type: none">• Telefonía interna.• Interconexión con la red de telefonía pública• Interconexión con la red de telefonía celular

La red corporativa tiene dos tipos de usuarios a los que presta servicios:

- **Usuarios internos:** Son aquellos usuarios que laboran dentro de la empresa y requieren de servicios de telecomunicaciones brindados por la red para el desempeño de sus actividades diarias.
- **Usuarios externos:** Son aquellos usuarios que no laboran en la empresa y que acceden a los servicios de red que la empresa publica en Internet, estos servicios están relacionados con el negocio y representan un ingreso económico importante.

3.2. Cálculo de la demanda.

La empresa cuenta con varias oficinas a nivel metropolitano que se distribuyen de la siguiente manera (ver figura 3.1):

- **Sede principal:** Es el centro de operaciones de la empresa, concentra la mayor cantidad de usuarios internos y por lo tanto la mayor demanda de servicios de red, en esta sede se ubica en datacenter de la red telecomunicaciones de la empresa.

- Sedes Secundarias: Son oficinas de apoyo a la sede principal, son un total de 3 sedes cercanas físicamente a la sede principal.
- Sedes Remotas: Son las oficinas que se encuentran localizadas en diferentes partes de la ciudad, estas sedes cumplen diferentes funciones; entre planta de producción, centro de capacitaciones, puntos de ventas, etc.

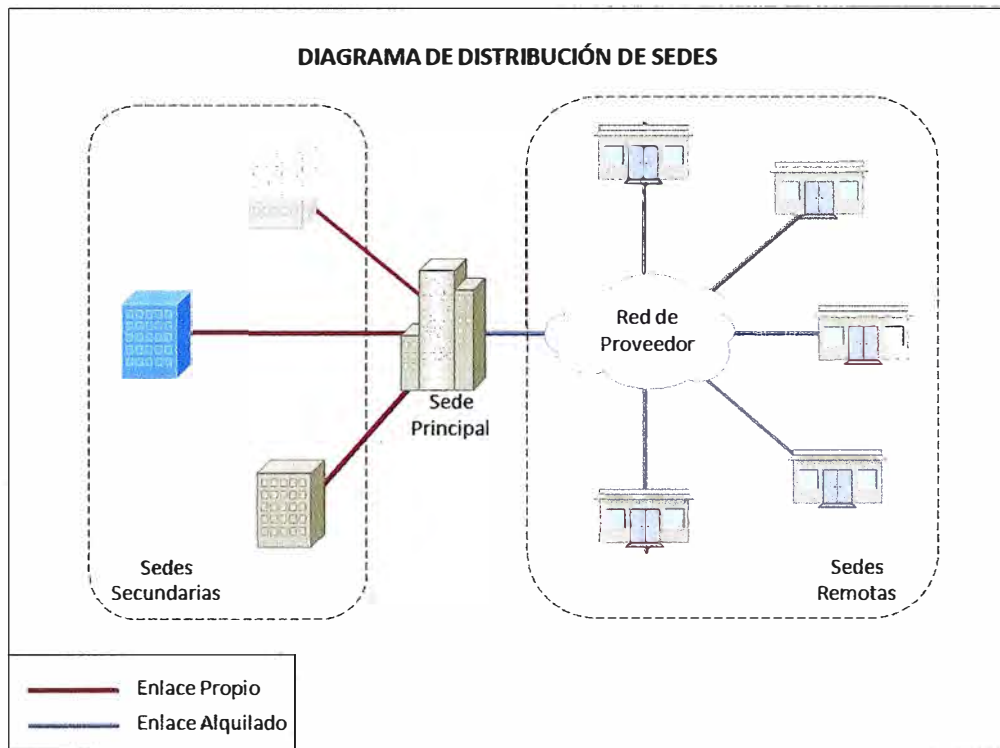


Figura 3.1 Diagrama de distribución de sedes

3.2.1. Consideraciones previas al cálculo de la demanda

Para un crecimiento en los próximos 5 años se considera lo siguiente:

- El número de usuarios de la red se incrementará en un 25% en los próximos 5 años.
- No todos los usuarios accederán a internet o usarán un teléfono IP, la demanda de estos servicios también se incrementará en un 25% en los próximos 5 años.
- Los servicios de la intranet, transferencias de archivos internos, correo electrónico interno y correo electrónico externo está permitido para todos los usuarios de la corporación, el incremento de la demanda de estos servicios está sujeto al incremento estimado para los usuarios que es del 25% en los próximos 5 años.
- En 5 años la corporación estima tener un máximo de 60 servidores publicados hacia internet, esto aparte de los servidores que brindan servicios a los usuarios internos.

En la tabla N° 3.2 se muestra la demanda de los servicios de la red de telecomunicaciones con una proyección de crecimiento de 5 años.

TABLA N° 3.2 Estimación de la demanda de la red de telecomunicaciones

Sede	Usuarios por sede	Navegación		Correo, intranet, transf. archivos		Telefonía	
		Usuarios con acceso a internet	Usuarios en 5 años con crecimiento de la demanda del 25%	Usuarios con acceso a correo	Usuarios en 5 años con crecimiento de la demanda del 25%	Número de teléfonos	Nº de teléfonos en 5 años con crecimiento de la demanda del 25%
Principal	1190	1071	1339	1190	1487,5	714	892,5
Sede Secundaria 1	270	243	304	270	337,5	162	202,5
Sede Secundaria 2	100	90	113	100	125	60	75
Sede Secundaria 3	100	90	113	100	125	60	75
Sede Remota 1	60	42	53	60	75	30	37,5
Sede Remota 2	60	42	53	60	75	30	37,5
Sede Remota 3	60	42	53	60	75	30	37,5
Sede Remota 4	30	21	26	30	37,5	9	11,25
Sede Remota 5	30	21	26	30	37,5	9	11,25
TOTAL	1900	1662	2080	1900	2375	1104	1380

Fuente: Elaboración propia

3.2.2. Consideraciones previas de diseño

- **Dimensionamiento de ancho de banda**

- Tasa de transferencia efectiva (TTE): Es el valor de la velocidad de transferencia que nos permite transferir una cantidad de información (bits) en un periodo de tiempo determinado (segundos).
- Tasa de transferencia nominal (TTN): Es el valor de la velocidad de transferencia indicada por el fabricante, por ejemplo, el cable UTP cat5 tiene una TTN de 100 Mbps.

Asumimos como condición de diseño, que la tasa de transferencia efectiva oscila entre el 35% a 40% de la tasa de transferencia nominal (TTN) dado que esto ocurre en la práctica para la gran mayoría de redes de datos tipo LAN y WAN.

Para el de diseño emplearemos la siguiente fórmula:

$$TTN = TTE \times 3 \quad (3.1)$$

- **Dimensionamiento de ancho de banda para telefonía IP**

Para calcular el ancho de banda generado por una llamada de IP a IP se empezará calculando el tamaño de las tramas de voz.

El tamaño de la trama es el resultado del CÓDEC utilizado. A esto debe sumarse el tamaño de los encabezados de las capas 4, 3 y 2, tal como se indica en la fórmula (3.2).

$$\text{Tamaño de la trama} = \text{Payload} + \text{Enc. 4} + \text{Enc. 3} + \text{Enc. 2} \quad (3.2)$$

Las tramas obtenidas al utilizar G.729 tienen una longitud de 20 Bytes, a eso debemos sumarle los encabezados RTP (8 Bytes), UDP (12 Bytes) e IP (20 Bytes) necesarios, que son 40 Bytes adicionales, luego debe sumarse el encabezado de capa de enlace; debido a empleamos la tecnología Ethernet la cabecera de la trama es de 18 Bytes, con lo cual se calcula el tamaño de la trama según se indica en la ecuación (3.3).

$$\text{Tamaño de la trama} = 20 \text{ Bytes} + 40 \text{ Bytes} + 18 \text{ Bytes} = 78 \text{ Bytes} \quad (3.3)$$

Dado el peso del encabezado en el tamaño de la trama a transmitir, es conveniente aplicar compresión de los encabezados de capa 3 y capa 4, lo que se suele denominar compresión de RTP (cRTP). Esto reduce esos 40 Bytes iniciales a solo 2 o 4 Bytes. De este modo nuestro cálculo queda:

$$\text{Tamaño de la trama} = 20 \text{ Bytes} + 2 \text{ Bytes} + 18 \text{ Bytes} = 40 \text{ Bytes} \quad (3.4)$$

A fin de continuar el cálculo, es necesario convertir el tamaño expresado en Bytes a bits.

$$\text{Tamaño de la trama} = 40 \times 8 = 320 \text{ bits} \quad (3.5)$$

Los códecs actualmente utilizados para la digitalización de voz (G.711, G.729) generan 50 tramas por segundo, para calcular el ancho de banda para cada llamada debemos multiplicar el tamaño de cada trama por la cantidad de tramas que se envían por segundo.

$$\frac{BW}{\text{llamada}} = (\text{Tamaño de la trama}) \times (\text{Tramas por segundo}) \quad (3.6)$$

Reemplazando valores en la ecuación (3.6) tenemos lo siguiente:

$$\frac{BW}{\text{llamada}} = (320) \times (50) \text{ bps} = 16 \text{ Kbps} \quad (3.7)$$

Este valor es el ancho de banda por cada llamada, el modo de calcular el ancho de banda requerido para el tráfico de telefonía IP se indica en la ecuación (3.8).

$$BW_{\text{Requerido}} = \left(\frac{BW}{\text{llamada}} \right) \times (N^{\circ} \text{ de llamadas concurrentes}) \quad (3.8)$$

- **Dimensionamiento de las llamadas concurrentes**

Dos o más llamadas son concurrentes cuando comparten un canal de comunicación al mismo tiempo.

En la tabla N° 3.3 se muestran los valores promedio de llamadas concurrentes de las sedes principales, secundarias y remotas y su estimación de crecimiento en 5 años, estos valores son promedios y no están sujetos a formulas, el incremento en 5 años está estimado en 25% del valor actual.

TABLA N° 3.3 Llamadas concurrentes

Sede	Llamadas concurrentes	
	Actuales	En 5 años
Sede Secundaria 1	20	25
Sede Secundaria 2	30	37,5
Sede Secundaria 3	30	37,5
Sede Remota 1	15	18,75
Sede Remota 2	15	18,75
Sede Remota 3	15	18,75
Sede Remota 4	4	5
Sede Remota 5	4	5

Fuente: Elaboración propia

- **Dimensionamiento del tráfico de llamadas externas**

Es común a nivel corporativo utilizar la unidad CCS (Cientos de segundos por hora). Una hora tiene 3600 segundos (36 CCS), entonces se establece la siguiente relación:

$$1 \text{ Erlang} = 36 \text{ CCS} \quad (3.9)$$

El tráfico promedio típico por usuario es de 0.17E (6 CCS), lo que corresponde a 10 minutos de conversación telefónica por hora. Típicamente este tráfico se divide en 50% interno y 50% externo, por lo tanto el tráfico por línea para llamadas externas es de 3 CCS.

Para calcular la cantidad de líneas necesarias, se debe tener en cuenta el tráfico externo y la “probabilidad de bloqueo”, la probabilidad de bloqueo es la probabilidad de que al desear realizar una llamada todas las líneas se encuentren ocupadas.

Asumiendo un tráfico promedio de un usuario al valor de 3 CCS tenemos lo siguiente:

$$\text{Tráfico externo} = (\text{Cantidad de teléfonos internos}) \times (3 \text{ CCS}) \quad (3.10)$$

Con el tráfico externo calculado en CCS, obtenemos el valor equivalente en Erlangs con la ecuación (3.9), para todos los casos consideraremos una probabilidad de bloqueo de 0.5 %, entonces calculamos el número de líneas troncales necesarias para nuestro tráfico en base a la tabla de distribución de Erlang B (anexo A).

3.2.3.Cálculo de la demanda de datos

- **Cálculo de la demanda de navegación a internet**

En base a lo mostrado en la tabla N° 3.2 tenemos que la cantidad de usuarios que cuentan con internet en la corporación es 2080 personas.

Un usuario promedio navega alrededor de 30 páginas web nuevas por día, cada página tiene un tamaño de 400 KBytes en promedio, por lo cual la cantidad de información transferida en un día es:

$$\text{Cantidad de información en un día} = 30 \times 400 \text{ Kbytes} = 12000 \text{ KBytes} \quad (3.11)$$

Convertimos el resultado de la ecuación (3.11) de Bytes a bits obteniendo lo siguiente:

$$\text{Cantidad de información en un día} = 96000 \text{ Kbits} \quad (3.12)$$

Consideramos que un día laborable tiene un promedio de 8 horas, esto equivale a 28800 segundos, entonces calculamos la tasa de transferencia efectiva (TTE):

$$TTE = \frac{\text{Cant.de información en un día}}{\text{Periodo de tiempo de un día}} = \frac{96000}{28800} (Kbps) \quad (3.13)$$

$$TTE = 3.33 Kbps \quad (3.14)$$

El valor TTE calculado en (3.14) es el correspondiente a tráfico promedio de navegación de un usuario, a fin de calcular el valor de la TTE para toda la corporación debemos multiplicar este número por la cantidad total de usuarios, que de acuerdo a la tabla N° 3.1 es igual a 2080.

$$TTE_{\text{Navegación}} = TTE \times (\text{Número de usuarios}) \quad (3.15)$$

Reemplazando valores tenemos:

$$TTE_{\text{Navegación}} = 3.33 \times 2080 = 6926.4 Kbps \quad (3.16)$$

Aplicamos la ecuación (3.1) para obtener el valor TTN para la navegación.

$$TTN_{\text{Navegación}} = 20.8 Mbps \quad (3.17)$$

Este ancho de banda calculado es el requerido para dar internet a todos los usuarios en la corporación, con un crecimiento de la demanda del 25% en 5 años.

• Cálculo de la demanda para servicios publicados en internet

Como se indico en las consideraciones previas al cálculo de la demanda, se estima llegar a tener un número de 60 servidores en la corporación que brinden servicios a usuarios externos.

Considerando que cada servidor publica una aplicación web con un peso promedio de 400 KBytes y que el promedio de visitas diaria es de 200 por página, se procederá al cálculo del valor de la TTE a fin de estimar la demanda de internet que requerimos para este servicio:

$$TTE_{\text{Serv.}} = \frac{(\text{N}^{\circ} \text{ de servidores}) \times (\text{Peso promedio en bits}) \times (\text{N}^{\circ} \text{ de visitas diarias})}{\text{Tiempo equivalente a un día}} \quad (3.18)$$

$$TTE_{\text{Serv.}} = 444.44 Kbps \quad (3.19)$$

Procedemos a calcular la TTN aplicando (3.1) para los servidores

$$TTN_{\text{Serv.}} = 1.33 Mbps \quad (3.20)$$

- **Cálculo de la demanda de correo electrónico externo**

Además del cálculo de la demanda de ancho de banda para internet se debe tener en cuenta el ancho de banda que se requiere para el envío y recepción de los correos electrónicos externos, estos son generados por los usuarios a través de sus cuentas de correo corporativas.

A diferencia de internet, el servicio de correo electrónico está habilitado para todos los usuarios de la red, diferenciamos dos tipos de tráfico, correo electrónico externo y correo electrónico interno.

En la tabla N° 3.4 se muestran los valores promedios de tráfico del correo electrónico externo para todas las sedes de la empresa.

TABLA N° 3.4 Valores promedio correo electrónico externo

Sede	Usuarios por sede	Usuarios en 5 años	Tamaño (KBytes)	Periodo (Horas)	TTE (Kbps)	TTN (Mbps)
Sede Principal	1190	1487,5	1000	8	413,19	1,24
Sede Secundaria 1	270	337,5	1000	8	93,75	0,28
Sede Secundaria 2	100	125	1000	8	34,72	0,10
Sede Secundaria 3	100	125	1000	8	34,72	0,10
Sede Remota 1	60	75	1000	8	20,83	0,06
Sede Remota 2	60	75	1000	8	20,83	0,06
Sede Remota 3	60	75	1000	8	20,83	0,06
Sede Remota 4	30	37,5	1000	8	10,42	0,03
Sede Remota 5	30	37,5	1000	8	10,42	0,03
					TTN correo ext. (Mbps)	1,98

Fuente: Elaboración propia

De acuerdo a la tabla N° 3.4 se considera que el tamaño del correo externo que envía o que recibe un usuario tiene un valor promedio de 1000 Kbytes.

Con las consideraciones indicadas, el ancho de banda de internet requerido para la corporación es:

$$BW_{Internet_{Total}} = TTN_{Navegación} + TTN_{Servidores} + TTN_{Correo\ ext.} \quad (3.21)$$

Reemplazando valores tenemos:

$$BW_{Internet_{Total}} = 24.11 \text{ Mbps} \quad (3.22)$$

- **Cálculo de la demanda de ancho de banda para las sedes remotas**

Las sedes secundarias y remotas se conectan a la sede principal a través de enlaces propios o arrendados a un proveedor de servicios de telecomunicaciones, por lo tanto se

calculará el ancho de banda necesario para estas las sedes a fin de determinar el valor de ancho de banda de los enlaces de comunicación que requerimos.

El tráfico que cursaría los enlaces de las sedes secundarias y remotas estaría conformado principalmente por lo siguiente:

✓ **Navegación de Internet**

En base a la TTE unitaria calculada en la ecuación (3.14) se procede a calcular la TTE total para cada sede y la TTN, tal como se indica en la tabla N° 3.5.

TABLA N° 3.5 Navegacion internet sedes secundarias y remotas

Sede	Usuarios con internet	Usuarios en 5 años	TTE (Kbps)	TTN (Mbps)
Sede Secundaria 1	243	303,75	1012,5	3,04
Sede Secundaria 2	90	112,5	375	1,13
Sede Secundaria 3	90	112,5	375	1,13
Sede Remota 1	42	52,5	175	0,53
Sede Remota 2	42	52,5	175	0,53
Sede Remota 3	42	52,5	175	0,53
Sede Remota 4	21	26,25	87,5	0,26
Sede Remota 5	21	26,25	87,5	0,26

Fuente: Elaboración propia

✓ **Cálculo de demanda para tráfico de correo electrónico interno**

El servicio de correo electrónico interno está disponible para todos los usuarios de la red. Se usa como promedio el valor de 1000 KBytes como tráfico de correo por día, los cálculos se muestran en la tabla N° 3.6.

TABLA N° 3.6 Correo electrónico interno sedes secundarias y remotas

Sede	Usuarios por sede	Usuarios en 5 años	Tamaño (KBytes)	Periodo (Horas)	TTE (Kbps)	TTN (Mbps)
Sede Secundaria 1	270	337,5	1000	8	93,75	0,28
Sede Secundaria 2	100	125	1000	8	34,72	0,10
Sede Secundaria 3	100	125	1000	8	34,72	0,10
Sede Remota 1	60	75	1000	8	20,83	0,06
Sede Remota 2	60	75	1000	8	20,83	0,06
Sede Remota 3	60	75	1000	8	20,83	0,06
Sede Remota 4	30	37,5	1000	8	10,42	0,03
Sede Remota 5	30	37,5	1000	8	10,42	0,03

Fuente: Elaboración propia

✓ Cálculo de demanda para tráfico de correo electrónico externo

El servicio de correo electrónico externo está habilitado para todos los usuarios de la red, se usa como promedio el valor de 1000 KBytes de tráfico de correo por día. Los cálculos se muestran en la tabla N° 3.7.

TABLA N° 3.7 Correo electrónico externo sedes secundarias y remotas

Sede	Usuarios por sede	Usuarios en 5 años	Tamaño (KBytes)	Periodo (Horas)	TTE (Kbps)	TTN (Mbps)
Sede Secundaria 1	270	337,5	1000	8	93,75	0,28
Sede Secundaria 2	100	125	1000	8	34,72	0,10
Sede Secundaria 3	100	125	1000	8	34,72	0,10
Sede Remota 1	60	75	1000	8	20,83	0,06
Sede Remota 2	60	75	1000	8	20,83	0,06
Sede Remota 3	60	75	1000	8	20,83	0,06
Sede Remota 4	30	37,5	1000	8	10,42	0,03
Sede Remota 5	30	37,5	1000	8	10,42	0,03

Fuente: Elaboración propia

✓ Cálculo de demanda para tráfico de Intranet

La intranet está habilitada para todos los usuarios, se estima que en promedio un usuario entra a 20 páginas de la intranet por día y que cada página tiene un tamaño promedio de 400 KBytes. Los cálculos se muestran en la tabla N° 3.8.

TABLA N° 3.8 Navegación intranet sedes secundarias y remotas

Sede	Usuarios por sede	Usuarios en 5 años	Tamaño total (KBytes)		Periodo (Horas)	TTE (Kbps)	TTN (Mbps)
			Nº pág.	Tam. pág.			
Sede Secundaria 1	270	337,5	20	400	8	750,00	2,25
Sede Secundaria 2	100	125	20	400	8	277,78	0,83
Sede Secundaria 3	100	125	20	400	8	277,78	0,83
Sede Remota 1	60	75	20	400	8	166,67	0,50
Sede Remota 2	60	75	20	400	8	166,67	0,50
Sede Remota 3	60	75	20	400	8	166,67	0,50
Sede Remota 4	30	37,5	20	400	8	83,33	0,25
Sede Remota 5	30	37,5	20	400	8	83,33	0,25

Fuente: Elaboración propia

✓ Cálculo de demanda para tráfico de transferencia de archivo

Todos los usuarios de la red pueden compartir archivos en repositorios comunes, como un servidor FTP, el promedio de tráfico transferido por el usuario para este servicio es de 500 KBytes por día. Los cálculos se muestran en la tabla N° 3.9.

TABLA N° 3.9 Transferencia de archivo sedes secundarias y remotas

Sede	Usuarios por sede	Usuarios en 5 años	Tamaño (KBytes)	Periodo (Horas)	TTE (Kbps)	TTN (Mbps)
Sede Secundaria 1	270	337,5	500	8	46,88	0,14
Sede Secundaria 2	100	125	500	8	17,36	0,05
Sede Secundaria 3	100	125	500	8	17,36	0,05
Sede Remota 1	60	75	500	8	10,42	0,03
Sede Remota 2	60	75	500	8	10,42	0,03
Sede Remota 3	60	75	500	8	10,42	0,03
Sede Remota 4	30	37,5	500	8	5,21	0,02
Sede Remota 5	30	37,5	500	8	5,21	0,02

Fuente: Elaboración propia

✓ Telefonía IP

Para el cálculo del tráfico que se genera en telefonía IP debemos tener en cuenta el ancho de banda por cada llamada realizada y el número de llamadas concurrentes promedio.

El ancho de banda que consume una llamada IP fue calculado en la ecuación (3.7), por otro lado el número de llamadas concurrentes promedio se obtiene de la tabla N° 3.3.

La tabla N°3.10 muestra los cálculos de TTE y TTN para la telefonía IP en las sedes secundarias y remotas.

TABLA N° 3.10 Telefonía IP sedes secundarias y remotas

Sede	Llamadas concurrentes		BW por llamada	TTE (Kbps)	TTN (Mbps)
	Actuales	En 5 años			
Sede Secundaria 1	20	25	16	400	1,20
Sede Secundaria 2	30	37,5	16	600	1,80
Sede Secundaria 3	30	37,5	16	600	1,80
Sede Remota 1	15	18,75	16	300	0,90
Sede Remota 2	15	18,75	16	300	0,90
Sede Remota 3	15	18,75	16	300	0,90
Sede Remota 4	4	5	16	80	0,24
Sede Remota 5	4	5	16	80	0,24

Fuente: Elaboración propia

Luego de realizar todos los cálculos, se muestra el consolidado de los resultados en la tabla N° 3.11 que es el ancho de banda estimado para cada uno de los enlaces que comunican las sedes secundarias y remotas con la sede principal.

TABLA N° 3.11 Ancho de banda total sedes secundarias y remotas

Sede	TTN						BW x sede (Mbps)
	Internet (Mbps)	Correo Int. (Mbps)	Correo Ext. (Mbps)	Intranet (Mbps)	Transf. Arch. (Mbps)	Tel. IP (Mbps)	
Sede Secundaria 1	3,04	0,28	0,28	2,25	0,14	1,2	7,19
Sede Secundaria 2	1,13	0,1	0,1	0,83	0,05	1,8	4,01
Sede Secundaria 3	1,13	0,1	0,1	0,83	0,05	1,8	4,01
Sede Remota 1	0,53	0,06	0,06	0,5	0,03	0,9	2,08
Sede Remota 2	0,53	0,06	0,06	0,5	0,03	0,9	2,08
Sede Remota 3	0,53	0,06	0,06	0,5	0,03	0,9	2,08
Sede Remota 4	0,26	0,03	0,03	0,25	0,02	0,24	0,83
Sede Remota 5	0,26	0,03	0,03	0,25	0,02	0,24	0,83

Finalmente hay que indicar que así como se contrata un enlace de un proveedor de servicio para las sedes remotas se debe contratar un enlace en la sede principal que sirva de puente de comunicación con las sedes remotas.

El ancho de banda que debe tener este enlace debe considerar la suma de todos los anchos de bandas de las sedes remotas, a fin de garantizar que aún en el caso que todos los enlaces estén siendo usados a su máximo valor no haya saturación en el canal.

Por lo tanto el ancho de banda del enlace a arrendar al proveedor para la sede principal debe tener un valor mínimo de:

$$BW_{princ.} = 2.08 + 2.08 + 2.08 + 0.83 + 0.83 = 7.9 \text{ Mbps} \quad (3.23)$$

3.2.4. Cálculo de la demanda de líneas telefónicas externas

Los usuarios en la red se encuentran distribuidos entre la sede principal, sedes secundarias y sedes remotas, la solución de telefonía estará centralizada en la sede principal, lo cual indica que las llamadas hacia la calle tendrán como recorrido la red de telecomunicaciones corporativa y saldrán a través del Gateway instalado en la sede principal.

Como se indica en la tabla N° 3.2 el número total de extensiones es de 1380.

Como segunda consideración se indica que el 100% de los usuarios que tienen teléfono podrán realizar llamadas externas y asimismo podrán recibirla.

En base a la ecuación (3.10) el valor del tráfico externo es:

$$\text{Tráfico externo} = (1380) \times (3 \text{ CCS}) = 4140 \text{ CCS} \quad (3.24)$$

Convirtiendo el valor obtenido en (3.24) a Erlangs tenemos lo siguiente:

$$4140 \text{ CCS} = 4140 \times \left(\frac{1}{36} \text{ Erlang}\right) = 115 \text{ Erlang} \quad (3.25)$$

Si queremos tener una probabilidad de bloqueo de 0.5 % en base a la tabla de distribución de Erlang B (Anexo A) tenemos:

$$115 \text{ E, a } 0.5\% \text{ de probabilidad de bloqueo} = 138 \text{ líneas externas} \quad (3.26)$$

Esta demanda se satisface con el empleo de 5 líneas primarias E1, dado que cada línea tiene capacidad de 30 canales, esto nos permite un total de hasta 150 líneas externas.

Con respecto a las llamadas a celulares consideramos que existe un grupo de usuarios que pueden llamar a celulares que en nuestro caso es el 25% de los usuarios que tienen teléfono IP; asumiendo que tenemos un tráfico de línea interna para llamadas a celular de 1 CCS, entonces aplicamos la fórmula (3.10) nuevamente:

$$\text{Tráfico externo} = (345) \times (1 \text{ CCS}) = 345 \text{ CCS} \quad (3.27)$$

Convirtiendo el valor obtenido a Erlangs obtenemos lo siguiente:

$$345 \text{ CCS} = 345 \times \left(\frac{1}{36} \text{ Erlang}\right) = 9.58 \text{ Erlang} \quad (3.28)$$

Si tenemos una probabilidad de bloqueo de 0.5 % en base a la tabla de distribución de Erlang B (Anexo A) obtenemos:

$$9.58 \text{ E a } 0.5\% \text{ de probabilidad de bloqueo} = 18 \text{ líneas externas} \quad (3.29)$$

En otras palabras requerimos de un gateway GSM con al menos 18 líneas externas para satisfacer la demanda de los usuarios que realizan llamadas a celulares, este valor contempla el crecimiento de la empresa para los próximos 5 años.

3.3. Interconexión de servicios con la red externa

Basados en los datos obtenidos en la sección anterior, podemos definir los servicios de la red como servicios internos y servicios externos.

Los servicios internos como su nombre lo indica son servicios brindados a los usuarios dentro de la red corporativa, es decir que el tráfico que se genera no sobrepasa los límites de la red corporativa.

Por otro lado, los servicios externos son aquellos que pueden ser generados dentro de la red e interactúan con algún elemento externo, para este caso el tráfico generado si sobrepasa las fronteras de la red corporativa.

En la tabla N° 3.12 se muestra la clasificación de los servicios dentro de la red de telecomunicaciones corporativa.

TABLA N° 3.12 Clasificación de los servicios de la red corp.

Navegación de Internet	Datos	Serv. Ext.
Correo electrónico externo		
Publicación de servicios web		
Telefonía con el exterior	Voz	
Navegación de Intranet	Datos	Serv. Int.
Transferencia de archivos en la red		
Correo electrónico interno		
Telefonía entre extensiones corporativas	Voz	

Fuente: Elaboración propia

Dado que tenemos calculada la demanda para todos estos servicios, debemos definir el modo de interconexión con la red externa.

3.3.1. Servicios externos – Datos

La interconexión de los servicios de datos en nuestra red debe ser a través de un equipo que sirva como punto de paso de todas las comunicaciones hacia el exterior, generalmente esto se hace a través de un equipo router propiedad de un proveedor de servicios de Internet (ISP).

Se tiene una única salida hacia internet básicamente por un tema de control y monitoreo, sin embargo a fin de aumentar la disponibilidad del servicio se puede tener un enlace de internet alternativo de menor capacidad o inclusive de la misma, que sirva como respaldo cuando el servicio del proveedor principal presente indisponibilidad. Recordando los valores de ancho de banda obtenidos en la sección anterior, procedemos a mostrarlos en la tabla N° 3.13:

TABLA N° 3.13 Servicios de datos externos

Servicio de datos externos	BW (Mbps)
Navegación de Internet	20,8
Publicación de servicios web	1,33
Correo electrónico externo	1,98
TOTAL	24,11

En valores comerciales requerimos arrendar un enlace de 27 Mbps a un ISP a fin de brindar los servicios de datos externos de manera normal teniendo en cuenta el crecimiento de la demanda en los próximos 5 años.

Cabe indicar que en base a los datos obtenidos se puede solicitar al proveedor ISP configurar calidad de servicio (QoS) en su equipo router a fin de tener reservado un ancho de banda para la publicación de servicios web, a un valor de 2 Mbps.

Es altamente recomendable que entre el equipo router del proveedor y la red corporativa, exista un equipo intermedio que se encargue de analizar los paquetes salientes y sobre todo entrantes que sirva para detectar algún posible ataque, estos equipos son los firewall, que por diseño se recomiendan que estén en clúster.

Por otro lado para el servicio de publicación web de los servidores de la empresa, se debe definir una zona en el firewall conocida como DMZ (Zona desmilitarizada) en la cual ubicar los servidores y que puedan recibir consultas desde la red externa sin comprometer la seguridad de la red corporativa.

En la figura 3.2 se muestra el detalle de la interconexión de servicios externos para datos.

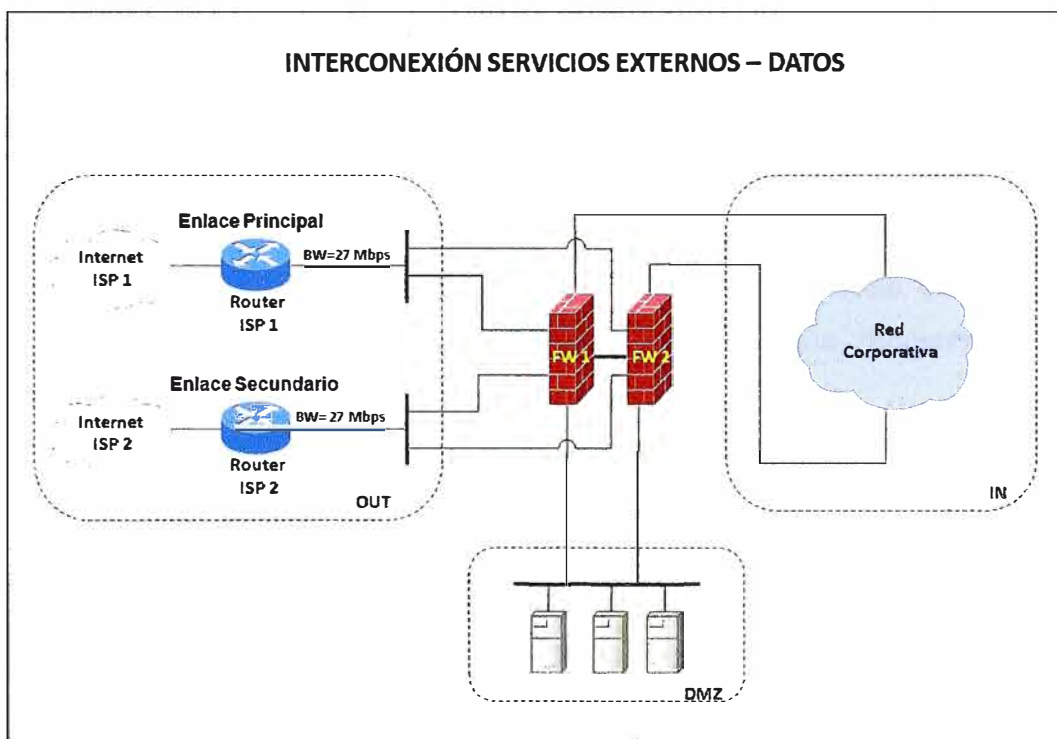


Figura 3.2 Interconexión servicios externos – datos

Como se puede apreciar en la figura 3.2 se están considerando dos enlaces de internet uno como contingencia del otro, El enlace secundario no debe tener necesariamente las mismas características que el enlace principal, es decir si el enlace principal llega con fibra óptica hasta el router del proveedor de servicios, para el enlace secundario podemos optar por un servicio de internet a través de un enlace de microondas que maneje el mismo ancho de banda; el costo del servicio de respaldo sería menor, además puede ser usado como un enlace para diferentes pruebas y no solo como contingencia.

Se puede apreciar además que a nivel de red corporativa existe redundancia de enlaces y de equipos, los firewall se encuentran en estado de clúster en modo de trabajo activo – activo y ante la falla de alguno de ellos el otro asumiría todas las funciones.

3.3.2. Servicios externos – Voz

En la sección 3.2.4 se calculó el número de líneas telefónicas externas necesarias para atender la demanda de los usuarios en la red corporativa, el resultado de los cálculos se muestran en la tabla N° 3.14

TABLA N° 3.14 Servicios de voz externos

Servicio de voz externos	Cantidad
Líneas externas para fijos	138
Líneas externas para celulares	18

En base a la tabla N°3.14 se debe contratar 5 líneas primarias E1 a un operador de telefonía, y se debe de contar también con un equipo Gateway GSM de al menos 18 canales para la telefonía celular.

Las líneas primarias E1 servirán para realizar llamadas a números fijos locales, nacionales y en caso sea necesario también a números internaciones, por otro lado se opta por un equipo Gateway GSM para llamadas a celular porque representa un ahorro significativo las llamadas a celulares dentro de la red GSM.

Físicamente la interconexión para el servicio de voz externo es un equipo router con tarjetería que soporte 5 líneas primarias E1 y un equipo gateway GSM con conexión IP que permita realizar llamadas a números celulares.

se considera tener dos equipos routers instalados para aumentar la disponibilidad del servicio de llamadas, cada equipo router debe soportar por lo menos 3 líneas primarias E1, de esta manera si alguno de estos equipos falla no se afecta el servicio. Por completo

A continuación en la figura 3.3 se muestra el detalle de la interconexión de servicios externos para la voz, los equipos routers están conectados a la red LAN de la empresa por un lado y por el otro lado tienen conexión a la red de telefonía pública (PSTN).

La solución de telefonía IP cuenta con dos centrales IPs que están en clúster en modo de trabajo activo-pasivo, esto aumenta la disponibilidad del servicio de telefonía IP, dado que si la central primaria presenta una falla, la central secundaria asume la continuidad del servicio. Asimismo se cuenta con un servidor para el servicio de casilla de voz, sin embargo podría estar todo incluido en un solo equipo junto con la central.

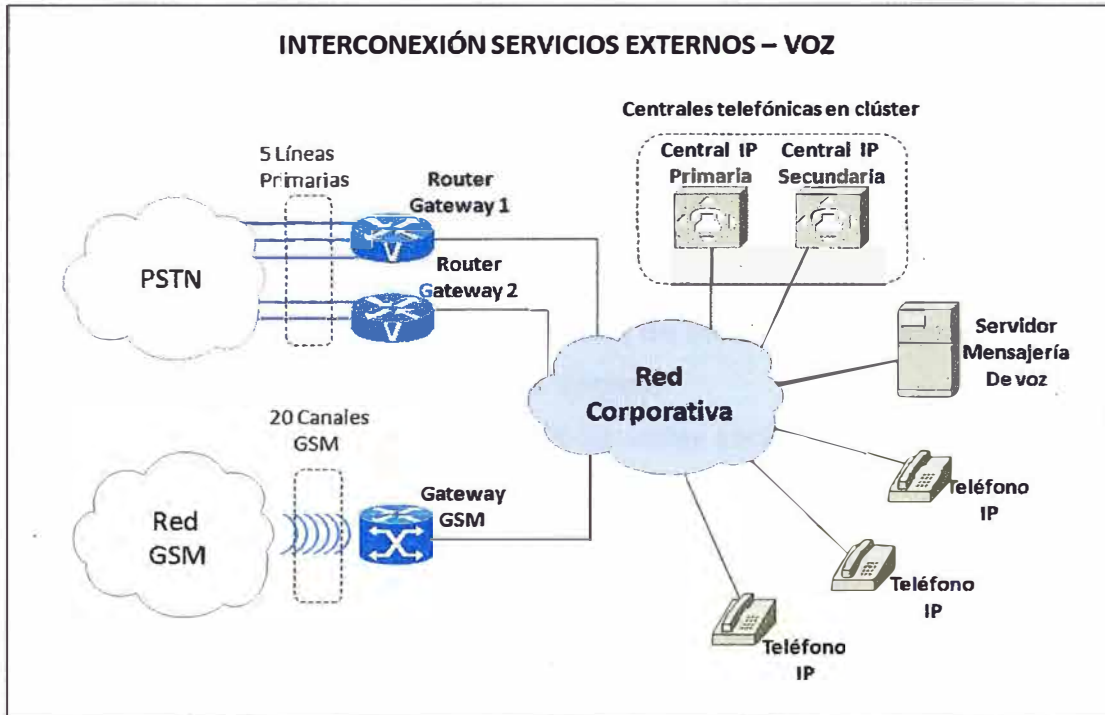


Figura 3.3 Interconexión servicios externos – voz

3.3.3. Interconexión de sedes secundarias y remotas

Es importante detallar la conectividad existente entre las sedes secundarias y la sede principal y la interconexión de las sedes remotas con la sede principal a través de la red de transporte del ISP.

El ancho de banda de conexión que se requiere para cada sede secundaria y remota se calculó en la sección anterior y se muestra en la tabla N° 3.15.

TABLA N° 3.15 Ancho de banda sedes secundarias

Sede	BW x sede (Mbps)	Valor Comercial (Mbps)
Sede Secundaria 1	7,19	10
Sede Secundaria 2	4,01	5
Sede Secundaria 3	4,01	5

Fuente: Elaboración propia

Para las sedes secundarias el escenario de conexión a la sede principal es el mismo para los tres casos, en todas existe un equipo de capa 3 que se encarga de realizar el enrutamiento a través del enlace físico (fibra óptica oscura) hacia el equipo de capa 3 de la sede principal (switch de núcleo), además todas las sedes secundarias tienen un enlace propio de respaldo que son radio enlaces que trabajan en la banda de frecuencia de los 5.4 GHz (banda libre).

Dado que la primera conexión es fibra óptica y es una conexión directa el ancho de banda disponible que existe entre las sedes secundarias y la sede principal está sujeto a la

electrónica de los equipos de capa 3 que son conectados entre sí, es decir a la velocidad de puerto a la que pueden llegar a trabajar, si tomamos en cuenta que 1 Gbps es la tasa de transferencia nominal para este enlace de fibra, entonces tendríamos una tasa de transferencia efectiva de aproximadamente 330 Mbps, lo cual comparado con el tráfico que se requiere no presenta problemas de saturación.

El valor del ancho de banda que brinda los radio enlaces se configura según indica la tabla N° 3.14, estos radio enlaces para el ancho de banda que manejan no representan un costo tan elevado y su mantenimiento es mínimo.

En la figura 3.4 se muestra la conectividad de las sedes secundarias con la sede principal:

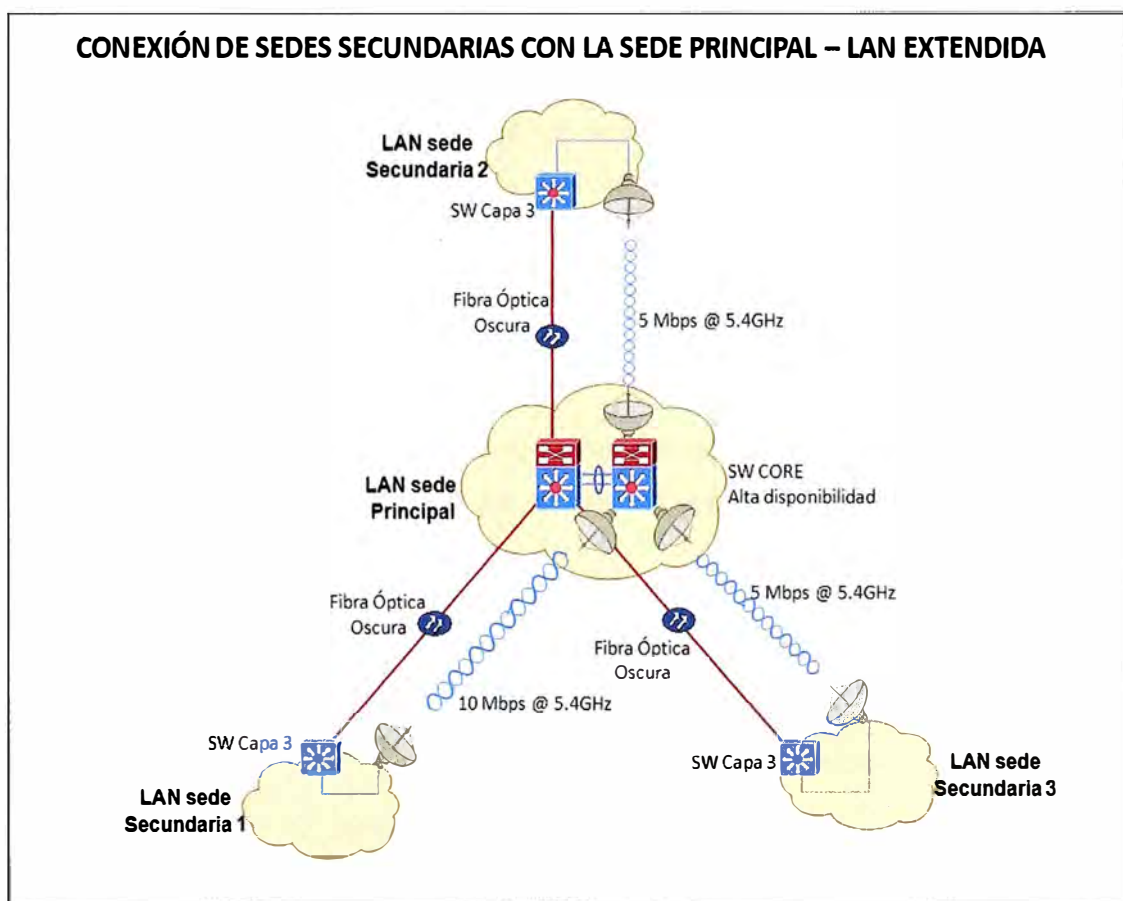


Figura 3.4 Conexión de sedes secundarias con la sede principal

En la figura 3.4 se muestra el modo de conexión entre las sedes secundarias y la sede principal, estas conexiones presentan redundancia de enlaces y de equipos, la red implementada satisface las necesidades de ancho de banda para cada una de estas sedes, dejando como líneas de respaldo los radios enlaces.

Por otro lado tenemos la conexión de las sedes remotas a la sede principal a través de la red de transporte de un ISP, la tecnología que usa el proveedor en su red de transporte para el cliente es transparente, en la tabla N° 3.16 se muestra el ancho de banda calculado para cada sede remota.

TABLA N° 3.16 Ancho de banda por sede remota

Sede	BW x sede (Mbps)	Valor Comercial (Mbps)
Sede Remota 1	2,08	3
Sede Remota 2	2,08	3
Sede Remota 3	2,08	3
Sede Remota 4	0,83	1.5
Sede Remota 5	0,83	1.5

Fuente: Elaboración propia

En base a la ecuación (3.23) tenemos el valor de ancho de banda de la sede principal igual a 7.9 Mbps.

Tomando como referencia un valor comercial decimos que el ancho de banda que debe tener la conexión en la sede principal debe ser de 10Mbps.

El punto de interconexión en cada una de las sedes remotas y en la sede principal es un router, generalmente de propiedad del proveedor el cual es la interfaz entre la red LAN local y la red de transporte del ISP, con la final de tener alta disponibilidad en las conexiones, el proveedor deja otro equipo router de las mismas características en estado de stand-by a fin de que actúe como respaldo en caso el router principal de una sede remota falle.

En la figura 3.5 se muestra el detalle de conexión entre las sedes remotas y la sede principal, asimismo se muestra el valor de ancho de banda para cada sede.

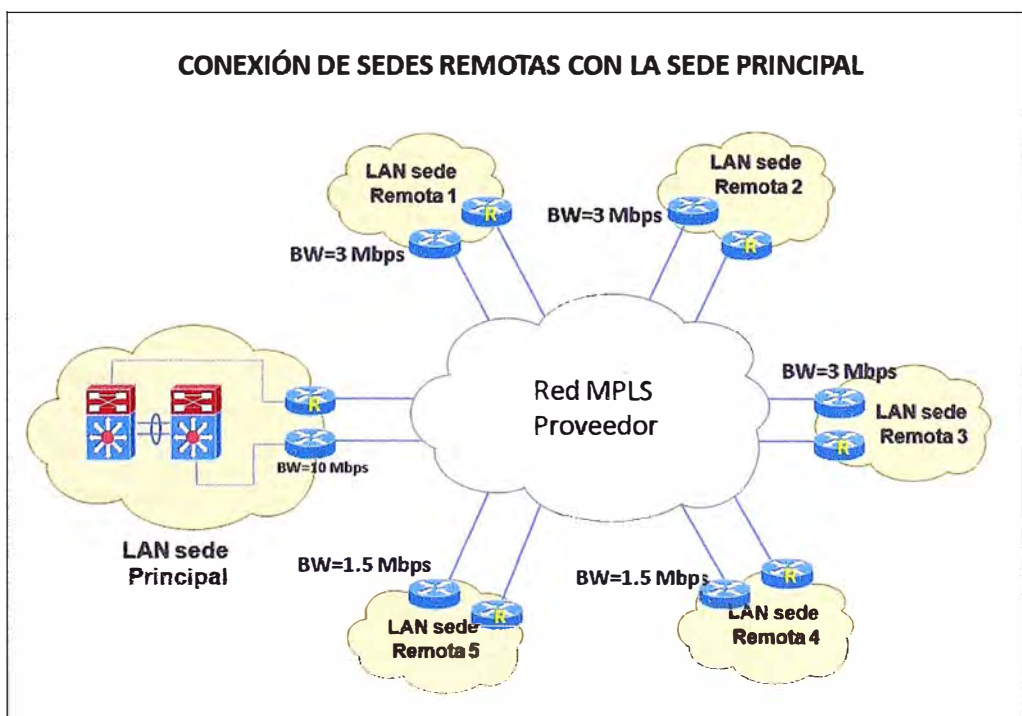


Figura 3.5 Conexión de sedes remotas con la sede principal.

CAPÍTULO IV INGENIERÍA DEL PROYECTO

4.1. Estructura de la red corporativa

La topología de la red que soportará los servicios de telecomunicaciones será del tipo jerárquica, con una capa de acceso de red para los usuarios y una capa de núcleo de alta conmutación.

Empezaremos por calcular el número de switches de acceso que se necesitan en la sede principal, para esto tomamos en cuenta que en el mercado existen principalmente switches de acceso con 24 y 48 puertos.

En la tabla N° 4.1 se muestra la cantidad de switches de acceso de 24 o de 48 puertos necesarios para atender la demanda de todos los usuarios de la sede principal.

TABLA N° 4.1 Número de equipos switches en sede principal

Ubicación	Usuarios	Crecimiento futuro	Puertos a instalar	N° equipos 48 puertos	N° equipos 24 puertos
Piso1	70	87,5	96	2	0
Piso2	100	125	144	3	0
Piso3	150	187,5	192	4	0
Piso4	150	187,5	192	4	0
Piso5	100	125	144	3	0
Piso6	100	125	144	4	0
Piso7	100	125	144	4	0
Piso8	150	187,5	192	3	0
Piso9	70	87,5	96	2	0
Piso10	70	87,5	96	2	0
Piso11	70	87,5	96	2	0
Piso12	60	75	96	2	0
Sala de datos (piso 7)	60	75	96	2	0
TOTAL	1250	1487,5	1728	37	0

Fuente: Elaboración propia

4.1.1. Capacidad de los switches de acceso

La capacidad requerida en la red de acceso es influenciada por dos elementos:

- Velocidad de los puertos de up-link
- Capacidad de conmutación

Para calcular los valores de velocidad de los puertos de up-link y la capacidad de conmutación, debemos estimar el consumo pico de ancho de banda por usuario, en la tabla N° 4.2 se indican los valores pico en función del servicio o actividad realizada.

TABLA N° 4.2 Requerimiento de ancho de banda pico por usuario

Servicios usados actualmente por los usuarios	Capacidad Pico (Mbps)
Navegación	0,200
Actualizaciones de sistema operativo	0,200
Actualizaciones de antivirus	0,200
Acceso a aplicación 1	2,000
Acceso a aplicación 2	2,000
Acceso a aplicación 3	2,000
Acceso a servidor de correo electrónico	1,000
Acceso a casilla de voz desde teléfono	1,000
Transferencias de archivos entre usuarios	25,000
Descargas de videos corporativos	5,000
Telefonía IP	0,016
Multiconferencia IP con 4 sesiones	0,060
Subtotal actual pico por usuario (Mbps)	38,676
Servicios requeridos en un futuro	Capacidad Pico (Mbps)
Aplicaciones colaborativas de audio y video	5,000
Video llamadas	1,000
Video conferencias con 4 sesiones	4,000
Ancho de banda reservado para aplicaciones posteriores	50,000
Subtotal adicional pico futuro por usuario (mbps)	60,000
Total de ancho de banda pico requerido por usuario (Mbps)	98,676

Fuente: Elaboración propia

De la tabla N° 4.2 se determina que el ancho de banda pico actual por usuario es de 38.676 Mbps, y que para un futuro se requerirá que el ancho de banda de la red soporte nuevas aplicaciones y servicios, por lo cual el ancho de banda pico requerido por usuario será de 60 Mbps, finalmente el ancho de banda pico total requerido por usuario viene dado por la suma de ambas cantidades dándonos el valor de 98.676 Mbps.

Para evitar posibles encolamientos y saturación en el puerto de red, los puertos de los switches de acceso deben tener un mínimo del doble de la capacidad calculada (191.8 Mbps), por lo tanto considerando valores comerciales, los puertos de los switches de acceso deben trabajar a 1 Gbps, dado que no existen equipos switches con puertos a 200 Mbps.

• Cálculo del enlace de up-link de los switches de acceso

Para calcular el valor del enlace de up-link definiremos el concepto de sobresuscripción, que relaciona la capacidad que un equipo tiene disponible en sus puertos up-link frente a la capacidad total que podría requerir en el peor de los casos (todos los puertos transmitiendo el máximo de tráfico al mismo tiempo).

$$\text{Relación de sobresuscripción} = \frac{(\text{N}^{\circ} \text{ de ptos.de acceso}) \times (\text{Capacidad de ptos.de acceso})}{\text{Capacidad de ptos.Up-link}} \quad (4.1)$$

Mientras más baja es la relación de sobresuscripción, mejor es el desempeño y la capacidad de crecimiento de los switches.

Según las consideraciones de diseño, la relación de sobresuscripción se puede clasificar de la siguiente manera:

- ✓ De 1:1 a 20:1, para las redes con un nivel de tráfico bajo.
- ✓ De 10:1 a 20:1, para redes con un nivel de tráfico medio-bajo, que utilizan la mayor parte del tiempo aplicaciones típicas.
- ✓ De 4:1 a 12:1, para las redes empresariales, con un nivel de tráfico medio utilizan aplicaciones típicas todo el tiempo y también aplicaciones especiales.
- ✓ De 5:1 a 10:1, para las redes empresariales con tráfico de servidores virtuales
- ✓ De 1:1 a 4:1, para las redes de data centers, con nivel de tráfico alto, que utilizan aplicaciones especiales todo el tiempo que requieren de un alto ancho de banda.

La red que estamos analizando es, en su gran mayoría, una red de usuarios finales con un tráfico típico, por tal motivo estimamos que la relación de sobresuscripción debe estar en el rango de 10:1 a 20:1.

Si consideramos que en un switch de acceso de 48 puertos Ethernet de 1Gbps, full dúplex todos sus puertos transmiten a su máxima velocidad en forma simultánea, la relación de sobresuscripción indica lo siguiente:

$$10 \leq \left(\frac{48 \text{ puertos} \times 2 \text{ Gbps}}{\text{Capacidad de puerto Uplink}} \right) \leq 20 \quad (4.2)$$

$$10 \leq \left(\frac{96 \text{ Gbps}}{\text{Capacidad de puerto Uplink}} \right) \leq 20 \quad (4.3)$$

Por lo tanto la capacidad de puerto up-link debe ser:

$$4.8 \text{ Gbps} \leq \text{Capacidad de puerto Up - link} \leq 9.6 \text{ Gbps} \quad (4.4)$$

Esto supone que nuestro enlace up-link entre la de red de acceso y los equipos de núcleo deben disponer de una capacidad entre 4.8 y 9.6 Gbps, por lo tanto se considera óptimo el empleo de un enlace up-link de 10 Gbps entre un switch de acceso y el switch de núcleo.

Debemos tomar en cuenta que en un área determinada (en este caso un piso), la red de acceso puede estar conformada no solo por un switch de acceso sino que puede estar conformada hasta por 4 equipos (ver tabla N° 4.1), por lo que cada switch de acceso debe contar con dos interfaces Ethernet de 10 Gbps cada uno.

- ✓ Una interface para la conexión al backbone de 10 Gbps
- ✓ Una interface para la conexión entre switches del mismo piso, para formar cascada o anillo local de 10 Gbps.

- **Cálculo de la capacidad de conmutación de los switches de acceso**

La capacidad de conmutación requerida para los switches de acceso se calcula considerando la transmisión simultánea full dúplex de todos sus puertos, es decir la suma de tráfico de todos los puertos Ethernet de 1 Gbps y los puertos de up-link de 10 Gbps.

$$CCSA = (NPUF) \times 2 \times (VPUF) + (NPU) \times 2 \times (VPU) \quad (4.5)$$

Donde:

CCSA: Capacidad de conmutación del switch de acceso

NPUF: Número de puertos de usuario final

VPUF: Velocidad del puerto de usuario final

NPU: Número de puertos Up-Link

VPU: Velocidad del puerto de Up-Link

Reemplazando valores en la ecuación (4.5) la capacidad de conmutación del switch de acceso de 48 puertos es:

$$CCSA = 48 \times 2 \times 1 \text{ Gbps} + 2 \times 2 \times 10 \text{ Gbps} = 136 \text{ Gbps} \quad (4.6)$$

En la tabla N° 4.3 se indica las capacidades mínimas que deben de tener los switches de acceso en la sede principal.

TABLA N° 4.3 Requisito switch de acceso

Cantidad de switches de acceso de 48 puertos	37
Capacidad de conmutación mínima para switch de acceso	136 Gbps
Número de puertos de F.O. a 10 Gbps, multi-modo, de up-link	2
Número de puertos RJ45, de 1 Gbps por switch	48

4.1.2. Capacidad de los switches de núcleo

La capa de núcleo es el backbone de alta velocidad de la red, la cual es crucial para permitir las comunicaciones dentro de la corporación; para calcular la capacidad de conmutación de los switches de núcleo se deben considerar lo siguiente:

• Tipo de topología o esquema de conexión

Debido a la cantidad de usuarios existentes y proyectados en la red de datos, es necesario instalar dos switches de núcleo conectados en topología redundante con modo de operación activo - activo, como se indica en la figura 4.1.

• Tipo de procesamiento

Elegimos para el diseño el tipo de switch modular, el cual realiza diferentes funciones de manera aislada en cada módulo todo dentro de un solo chasis, cada módulo cuenta con un procesamiento independiente para un mejor rendimiento, luego los módulos dentro del chasis del núcleo se integran a través de buses de alta velocidad.

• Cantidad y tipo de puertos

Para el cálculo de la cantidad y tipo de puertos en el switch de core se debe tener en cuenta los siguientes aspectos:

- Las conexiones de fibra óptica, multi-modo a 10 Gbps con los switches de acceso.

- Las conexiones de fibra óptica, multi-modo a 10 Gbps con los servidores
- La interconexión de fibra óptica, multi-modo a 10 Gbps entre switches de núcleo.
- Las conexiones de fibra óptica y RJ45 a 1Gbps con los servidores y los equipos de comunicaciones del centro de cómputo.
- Respaldo de cada tipo de puertos.
- Los puertos se distribuyen de forma balanceada para los dos switches de núcleo.

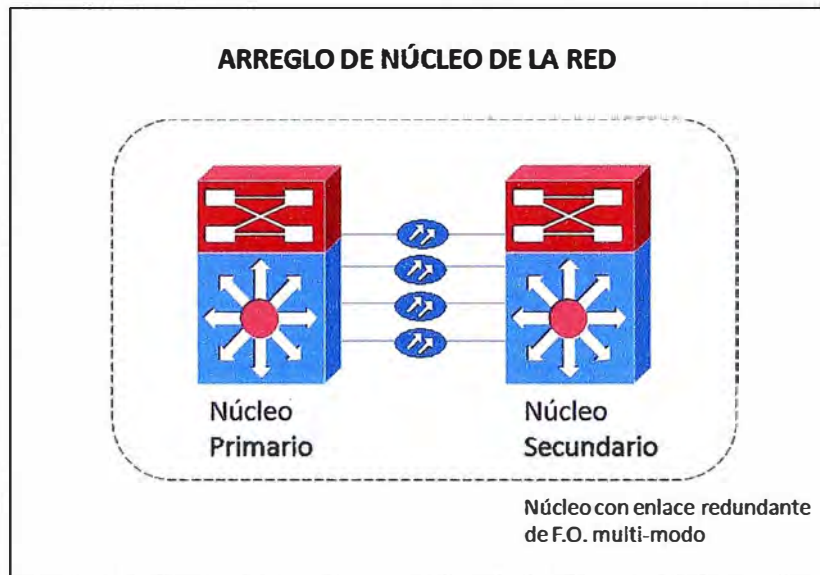


Figura 4.1 Arreglo de núcleo de la red

Consideramos que la conexión entre los switches de núcleo está dada por 4 enlaces de F.O., multi-modo a 10 Gbps tal como se muestra en la figura 4.1, además debe tener las siguientes características:

- Alta disponibilidad.
- Brindar redundancia.
- Brindar tolerancia a fallos.
- Adaptabilidad rápida a cambios.
- Ofrecer baja latencia y buena gestión.
- Alta velocidad de conmutación.
- Manejo de gran cantidad de información.
- Capacidad de enrutamiento a nivel de capa 3.

Para uso futuro se contempla la necesidad de tener servidores con conexión de 10Gbps con redundancia, por tal motivo consideramos 5 conexiones adicionales de 10 Gbps de F.O. multi-modo para los servidores, en la tabla N° 4.4 se muestra la cantidad y tipo de puertos necesarios en ambos switches de núcleo.

TABLA Nº 4.4 Cantidad y tipo de puertos en los switches de núcleo

Ubicación	Nº Equipos 48 Puertos	SWITCH NÚCLEO PRIMARIO				SWITCH NÚCLEO SECUNDARIO			
		Puertos F.O. a 10 Gbps Backbone	Puertos F.O. a 10 Gbps Servidores	Puertos F.O. a 1 Gbps Servidores	Puertos RJ45 a 1 Gbps para equipos varios	Puertos F.O. a 10 Gbps Backbone	Puertos F.O. a 10 Gbps Servidores	Puertos F.O. a 1 Gbps Servidores	Puertos RJ45 a 1 Gbps para equipos varios
Piso1	2	1				1			
Piso2	3	1				1			
Piso3	4	1				1			
Piso4	4	1				1			
Piso5	3	1				1			
Piso6	4	1				1			
Piso7	4	1				1			
Piso8	3	1				1			
Piso9	2	1				1			
Piso10	2	1				1			
Piso11	2	1				1			
Piso12	2	1				1			
Sala de datos	2	1	5		48	1	5		48
Interconexión entre switches		4				4			
Respaldo		3	3			3	3		
TOTAL		20	8		48	20	8		48

Tomando en cuenta las consideraciones anteriores y en base a la información que se muestra en la tabla N°4.4 calculamos la capacidad de conmutación de los switches de núcleo considerando el tráfico que se genera dependiendo del tipo de puerto o función que realiza el switch de núcleo, esto se indica a continuación:

- El tráfico de todos los puertos de fibra óptica, multi-modo a 10 Gbps.
- El tráfico de todos los puertos de fibra óptica, multi-modo a 1 Gbps.
- El tráfico de todos los puertos RJ45 de 1 Gbps.
- El tráfico de las funciones adicionales, por ejemplo firewall, supervisión, etc.
- Tráfico futuro de los slots vacíos para el crecimiento.
- Capacidad total de los puertos para transmisión full dúplex.

Para los tres primeros puntos, en base a la información de la tabla N° 4.4 obtenemos la capacidad total de conmutación para los puertos de red del Núcleo que se muestra en la tabla N° 4.5.

TABLA N° 4.5 Capacidad total de conmutación para los puertos de red del Núcleo

	Total	Capacidad de conmutación(Gbps)
Puertos F.O. a 10 Gbps Backbone	20	400
Puertos F.O. a 10 Gbps Servidores	8	160
Puertos RJ45 a 1 Gbps para equipos varios	48	96
Capacidad total de conmutación para los puertos de red del Núcleo (Gbps)		656

Procederemos a calcular el número de tarjetas necesarias para cubrir la cantidad de puertos en función a la velocidad, este cálculo se muestra en la tabla N° 4.6.

TABLA N° 4.6 Número de tarjetas necesarias en función de la velocidad

	Total puertos	Número de puertos por tarjeta	Número de tarjetas
Puertos F.O. a 10 Gbps	28	16	2
Puertos RJ45 a 1 Gbps	48	48	1

Para el cálculo de la capacidad de conmutación de las demás tarjetas la tabla N° 4.7 muestra los siguientes valores promedios considerados.

TABLA N° 4.7 Capacidades estimadas de conmutación

	Capacidad de conmutación(Gbps)	N° de tarjetas estimadas
Capacidad de conmutación para tarjeta supervisora	80	1
Capacidad de conmutación para funciones especiales	80	1

Tendríamos 5 tarjetas dentro del chasis del switch de núcleo; finalmente debemos calcular la capacidad de conmutación correspondiente a los slots que dejaríamos vacío, consideremos un crecimiento del 25% sobre la cantidad actual de tarjetas que tiene el Núcleo, entonces el número de slots destinado para crecimiento sería:

$$\text{Número de slot crecimiento} = (25\%) \times (\text{Número de tarjetas}) \quad (4.7)$$

$$\text{Número de slot crecimiento} = (25\%) \times (5) = 1.25 \quad (4.8)$$

Por lo tanto consideramos el valor de 2 slots vacíos destinados para uso futuro, a continuación de la misma manera que se consideró para las tarjetas de funciones especiales, para estos slots se considerara una capacidad de conmutación promedio de 80 Gbps, estas dos tarjetas de crecimiento futuro generarían una capacidad de conmutación de 160 Gbps, en la tabla N° 4.8 se muestra la capacidad de conmutación total requerida para el equipo de núcleo.

TABLA N° 4.8 Capacidades de conmutación total del switch Núcleo

	Capacidad de conmutación (Gbps)	Número de tarjetas
Capacidad de conmutación para los puertos de red	656	3
Capacidad de conmutación para tarjeta supervisora	80	1
Capacidad de conmutación para funciones especiales	80	1
Capacidad de conmutación slots vacíos de crecimiento	160	2
TOTAL	976	7

Luego de realizar el cálculo de dimensionamiento concluimos que nuestros switches de núcleo deberán contar con los requisitos indicados en la tabla N° 4.9.

TABLA N° 4.9 Requisitos mínimos de los switches de núcleo

Requisito	Switch núcleo primario	Switch núcleo secundario
Tipo de arquitectura	Modular	Modular
Número de slots mínimo	7	7
Capacidad de conmutación mínima	976 Gbps	976 Gbps
Supervisora	1	1
Número de puertos de F.O. a 10 Gbps, Multi-modo	28	28
Número de puertos RJ45, de 1Gbps	48	48
Modo de Operación	Activo-Activo	Activo-Activo

4.1.3. Red de acceso

La red de acceso es el equipamiento de la red más cercano al usuario, en la mayoría de redes LAN la conexión a la red de acceso para el usuario es a través del cableado horizontal de la red corporativa.

La conectividad física a la red de acceso empieza desde la interfaz de red de la estación de trabajo del usuario, pasando por el cableado estructurado horizontal hasta el puerto del switch de acceso del rack de comunicaciones, de esta manera podemos acceder a todos los servicios de la red corporativa.

Los switches de la redes de acceso no solo conectan PCs de usuarios sino que, debido a las crecientes necesidades de servicios Power over Ethernet (PoE) en redes corporativas, también conectan teléfonos IP, puntos de acceso inalámbrico, etc., por lo cual es cada vez más frecuente el uso de switches que además de cumplir con los requisitos indicados tengan habilitado en cada puerto el servicio de PoE que se indica en la especificación 802.3af de la IEEE.

- **Conexión de la capa de acceso con la capa de núcleo – sede principal**

Con la finalidad de tener una red redundante y tolerable a fallas, se realizará la conexión de los switches de acceso hacia el núcleo basados en el protocolo STP (IEEE 802.1D), este protocolo permite tener una topología física cerrada y asegura una topología lógica libre de bucles.

En la sede principal la cantidad de switches instalados en un rack de comunicaciones varía por piso, por ejemplo los pisos 1, 9, 10, 11, 12 y la sala de datos cuentan con dos switches de accesos, en la figura 4.2 se muestra el modo de conexión de los switches de acceso al núcleo.

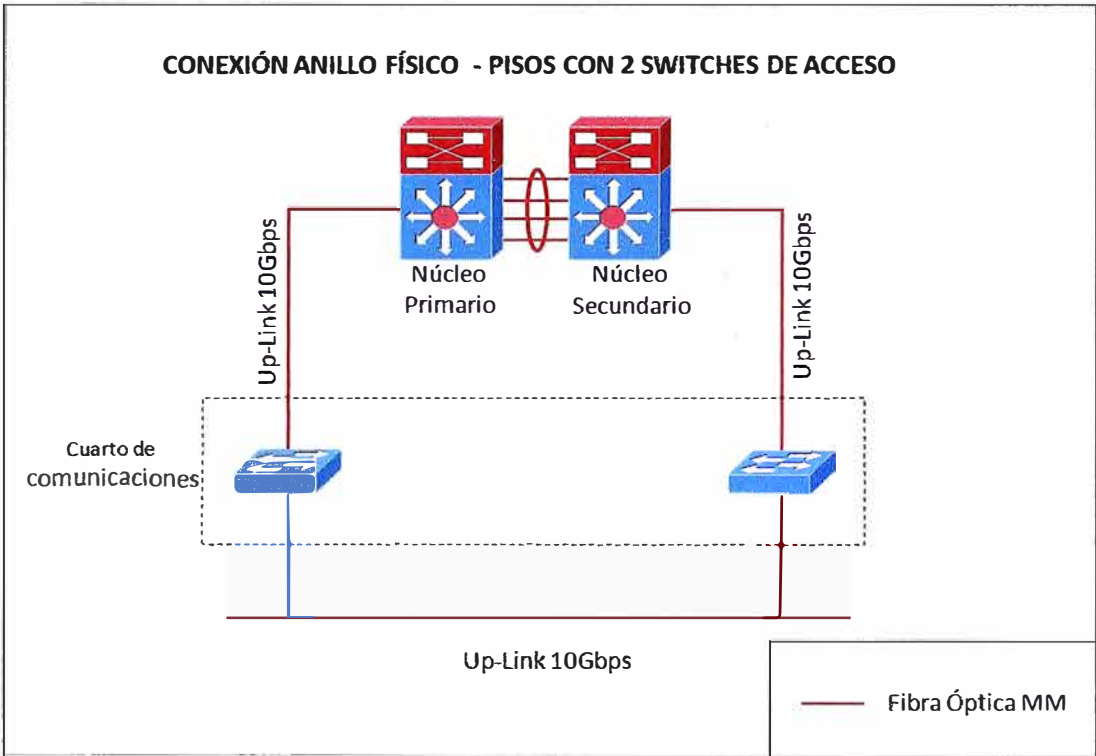


Figura 4.2 Conexión anillo físico – pisos con 2 switches de acceso

De la misma manera se realiza la conexión de los switches de acceso en los pisos 2, 5 y 8 que cuentan con 3 switches en su cuarto de comunicaciones, para este caso el modo de conexión de los switches de acceso al núcleo se muestra en la figura 4.3.

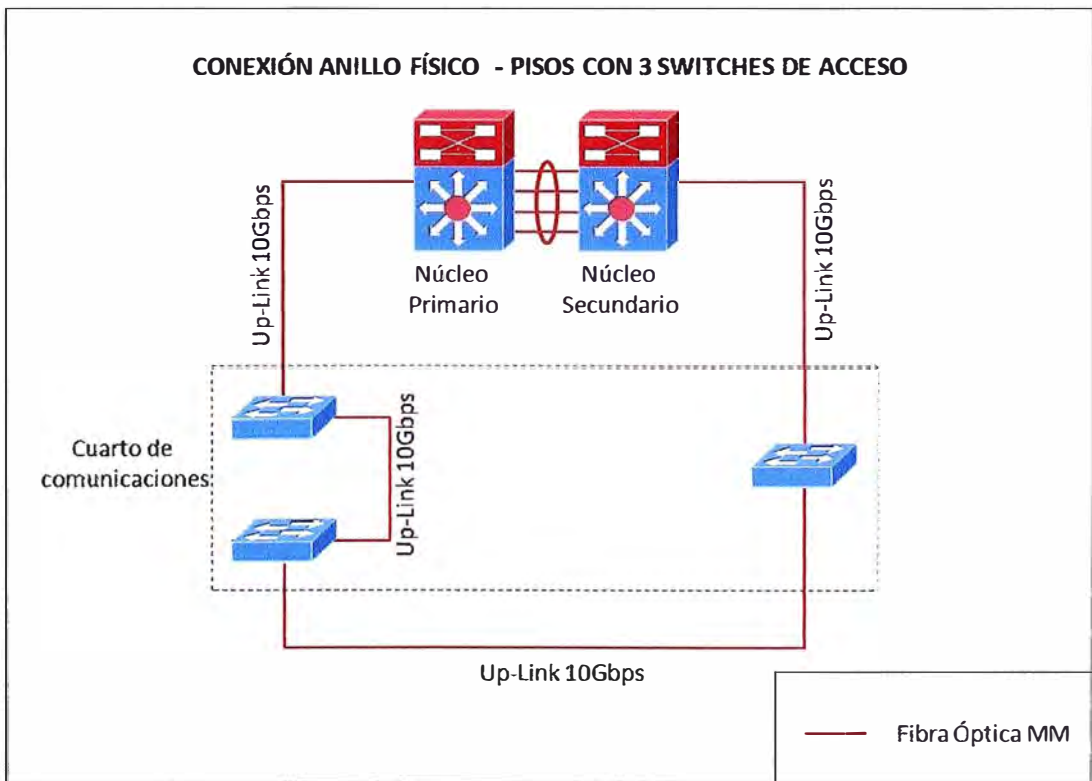


Figura 4.3 Conexión anillo físico – pisos con 3 switches de acceso

Los pisos 3, 4, 6 y 7 cuentan con 4 switches de acceso en sus respectivos cuartos de comunicaciones, para este caso el modo de conexión de los switches de acceso al núcleo se muestra en la figura 4.4.

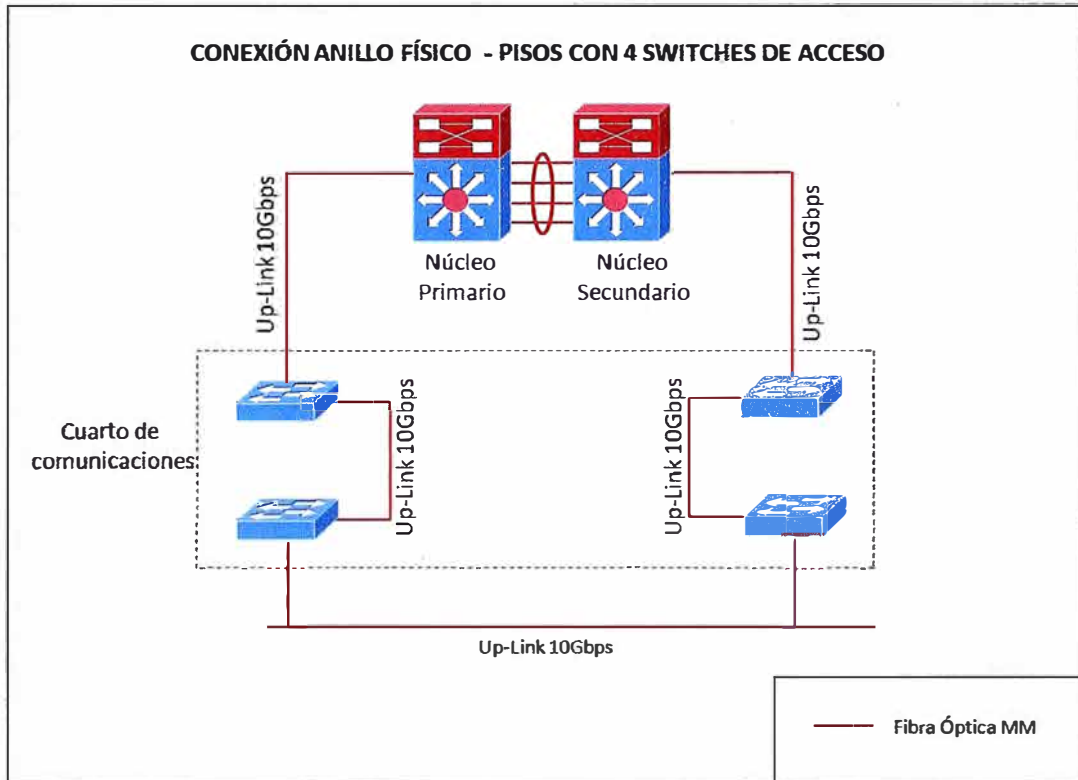


Figura 4.4 Conexión anillo físico – pisos con 4 switches de acceso

4.1.4. Otro tipo de redes de acceso

•Consideraciones previas

En la sección 4.1.3 se indicó el modo de conectividad de la LAN de la sede principal, sin embargo las sedes secundarias y remotas son a su vez redes LAN independientes las cuales acceden a los recursos y servicios ubicados en la red sede principal.

Si bien las sedes secundarias y remotas cuentan con los mismos servicios que los usuarios en la sede principal, existen políticas que restringen el tráfico hacia algún segmento de la LAN principal desde las sedes secundarias y remotas, por ejemplo se configuran listas de acceso en los equipos de capa 3 (switches o routers) a fin de controlar el tráfico de las sedes secundarias y remotas para que solo accedan a los servicios que realmente requieren para sus actividades diarias.

Debido a que la cantidad de usuarios en cada una de las sedes secundarias y remotas es mucho menor que en la sede principal y además por políticas de acceso no llegarán a generar el mismo tráfico que los usuarios de la sede principal, consideraremos un ancho de banda de acceso de 100 Mbps por usuario.

Para las sedes secundarias que se conectan directamente a la red LAN principal debemos considerar un equipo de capa 3 con nivel de enrutamiento que sea capaz de establecer comunicación con el switch de núcleo de la sede principal, la razón de tener un equipo de capa 3 entre estas sedes es de reducir el número de tormentas de broadcast y no perjudicar el rendimiento de la red tanto local como general.

En primer lugar calculamos la cantidad de equipos switches necesarios en las sedes secundarias y remotas, en la tabla N°4.10 se muestra este resultado.

TABLA N° 4.10 Cantidad de equipos switches en las sedes secundarias y remotas

Sede secundaria 1		Crecimiento futuro	Puertos a instalar (24/48)	N° equipos 48 puertos	N° equipos 24 puertos
Ubicación	Usuarios				
Piso1	100	125	144	3	0
Piso2	70	87,5	96	2	0
Piso3	100	125	144	3	0
TOTAL	270	337,5	384	8	0
Sedes remotas		Crecimiento futuro	Puertos a instalar (24/48)	N° equipos 48 puertos	N° equipos 24 puertos
Ubicación	Usuarios				
Sede Secundaria 2	100	125	168	2	1
Sede Secundaria 3	100	125	168	2	1
Sede Remota 1	60	75	96	2	0
Sede Remota 2	60	75	96	2	0
Sede Remota 3	60	75	96	2	0
Sede Remota 4	30	37,5	48	1	0
Sede Remota 5	30	37,5	48	1	0
TOTAL	440	550	720	12	2

Fuente: Elaboración propia

• Cálculo de los requisitos – sede secundaria 1

Con las consideraciones previas indicadas, se calcula los requisitos necesarios para los switches de acceso de la sede secundaria 1 asimismo se calcula los requisitos necesarios para el equipo de capa tres que tendrá conectividad con el switch de núcleo de la sede principal.

- Switches de acceso – Sede secundaria 1

En la tabla N° 4.10 se muestra que se requieren 8 switches de acceso de 48 puertos cada uno, con cada puerto a la velocidad de 100 Mbps en full dúplex, entonces utilizando la ecuación (4.1) se calcula la velocidad del puerto up-link basado en la relación de sobreescripción.

Luego del desarrollo encontramos que la capacidad de puerto up-link para los switches de acceso de la sede secundaria 1 debe ser:

$$480 \text{ Mbps} \leq \text{Capacidad de puerto Up - link} \leq 960 \text{ Mbps} \quad (4.9)$$

Tomamos el valor de 1 Gbps como capacidad de puerto up-link ya que los switches de manera comercial tienen puertos de up-link a esa velocidad, por otro lado el equipo switch de acceso de la sede secundaria 1 debe tener:

- Una interface up-link de 1Gbps.
- Una interface para la conexión entre switches del mismo piso, para formar cascada o anillo local de 1 Gbps.

Para el cálculo de la capacidad de conmutación de los switches de accesos de la sede secundaria 1 utilizaremos la ecuación (4.5) definida anteriormente, al reemplazar valores tenemos lo siguiente:

$$CCSA = 48 \times 2 \times 100 \text{ Mbps} + 2 \times 2 \times 1000 \text{ Mbps} = 13.6 \text{ Gbps} \quad (4.10)$$

En la tabla N°4.11 se muestra los requerimientos mínimos de los switches de acceso en la sede secundaria 1.

TABLA N° 4.11 Requisitos mínimos de los switches de acceso sede secundaria 1

Requisito	Switch de acceso
Cantidad de switches de acceso	8
Capacidad de conmutación mínima para switch de acceso	13.6 Gbps
Número de puertos de F.O. a 1 Gbps, multi-modo, de up-link	1
Número de puertos de RJ45 a 1 Gbps de up-link	1
Número de puertos RJ45, de 100 Mbps	48

- Switch de capa 3 – Sede secundaria 1

A diferencia de un switch de acceso en donde los valores de velocidad de up-link y la capacidad de conmutación se calculan en base a todos sus puertos, en el switch de capa tres se debe notar que no usa todos los puertos y solo recibe tráfico de las conexiones de los switches de acceso.

En la figura 4.5 se muestra la topología de red de la sede secundaria 1, en base a esta figura el cálculo se hará en función solo a seis puertos.

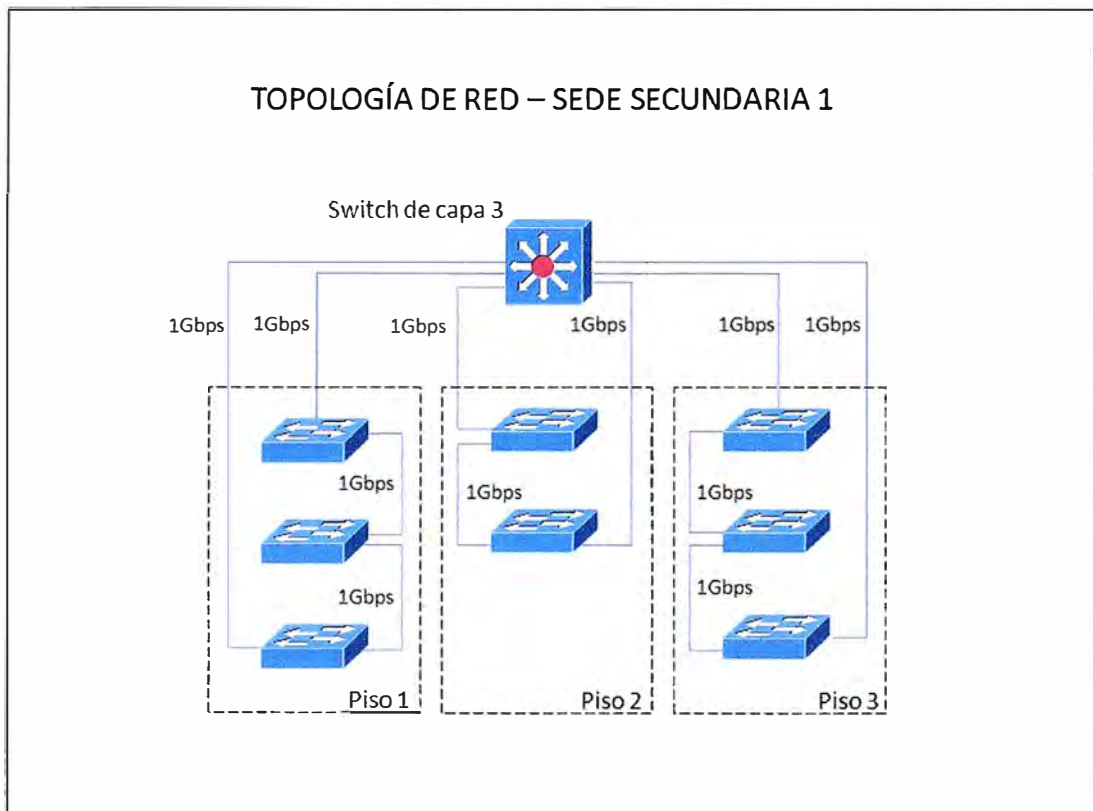


Figura 4.5 Topología de red sede secundaria 1

En base a la ecuación (4.1), y usando el valor de relación de sobresuscripción se calcula la capacidad del puerto up-link para el switch de capa 3 de la sede secundaria 1.

$$0,6 \text{ Gbps} \leq \text{Capacidad de puerto Up – link} \leq 1,2 \text{ Gbps} \quad (4.11)$$

En base a lo obtenido para el valor de up-link, consideramos 1 Gbps como la capacidad del puerto que conecta el switch de capa 3 de la sede secundaria 1 con el switch de núcleo en la sede principal, por lo tanto nuestro equipo switch de capa 3 debe tener:

- Una interface up-link, RJ45, de 1 Gbps para la conexión al switch de núcleo.
- Una interface up-link, RJ45, de 1 Gbps para la conexión de respaldo.

El otro valor que requerimos dimensionar es el de la capacidad de conmutación, para este caso se usará la ecuación (4.5), de donde obtenemos después del reemplazo de valores lo siguiente:

$$CCSA = 6 \times 2 \times 1 \text{ Gbps} + 2 \times 2 \times 1 \text{ Gbps} = 16 \text{ Gbps} \quad (4.12)$$

En la tabla N°4.12 se muestra las capacidades mínimas que deben tener los switches de capa 3 de la sede secundaria 1.

TABLA N° 4.12 Requisitos mínimos de los switches capa 3 sede secundaria 1

Requisito	Switch de capa 3
Cantidad de switches de capa 3	1
Capacidad de conmutación mínima	16 Gbps
Número de puertos de F.O. a 1 Gbps, multi-modo, de up-link	4
Número de puertos RJ45, a 1 Gbps	24

En la figura 4.6 se muestra la topología total para la sede secundaria 1, además se muestra el detalle de conexión con la sede principal.

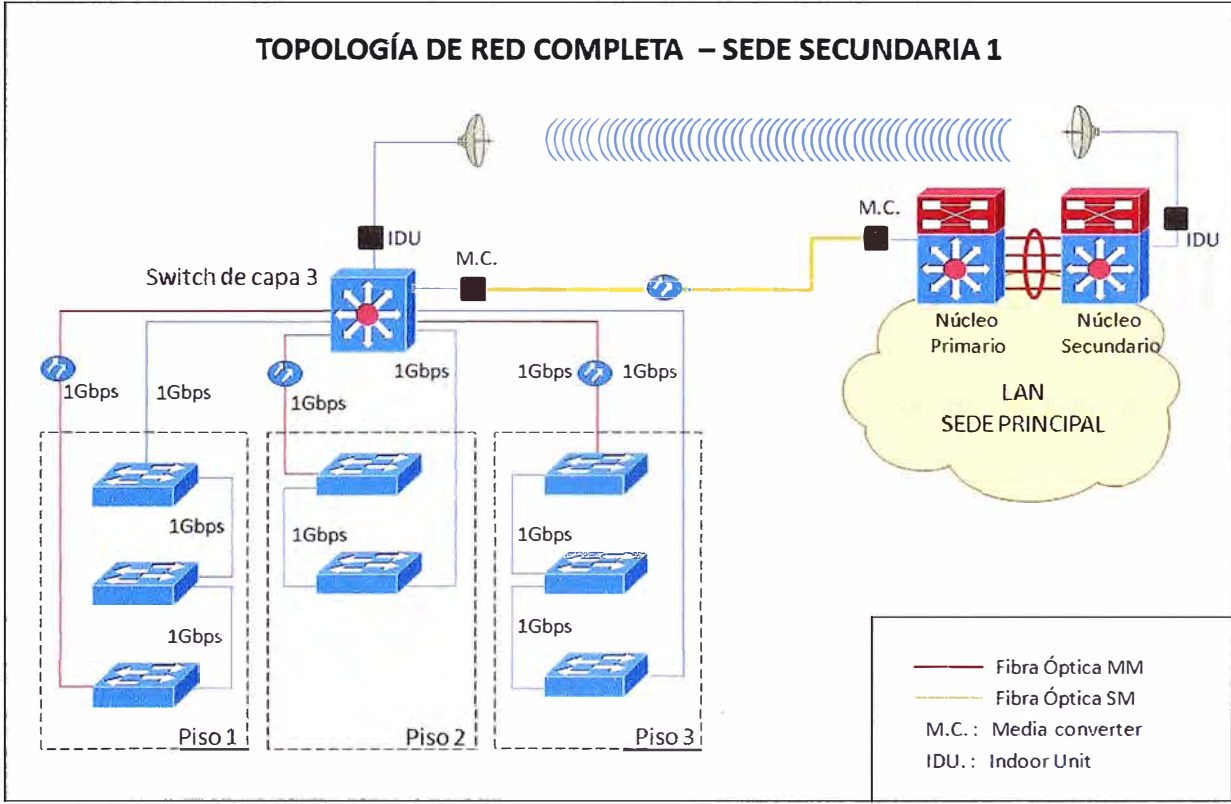


Figura 4.6 Topología de red completa – sede secundaria 1

• **Cálculo de los requisitos – sedes secundarias 2 y 3**

Las sedes secundarias 2 y 3 requieren del mismo número de equipos de acuerdo a la tabla 4.10, Ambas sedes cuentan con dos switches de acceso de 48 puertos y un switch de acceso de 24 puertos haciendo un total de 3 switches, todos trabajando a una velocidad de puerto de 100 Mbps full dúplex.

En la figura 4.7 se muestra la topología de red completa para las sedes secundarias 2 y 3, además se muestra el detalle de conexión con la sede principal; como se indicó anteriormente ambas sedes cuentan con el mismo esquema de red y con el mismo esquema de conexión a la sede principal.

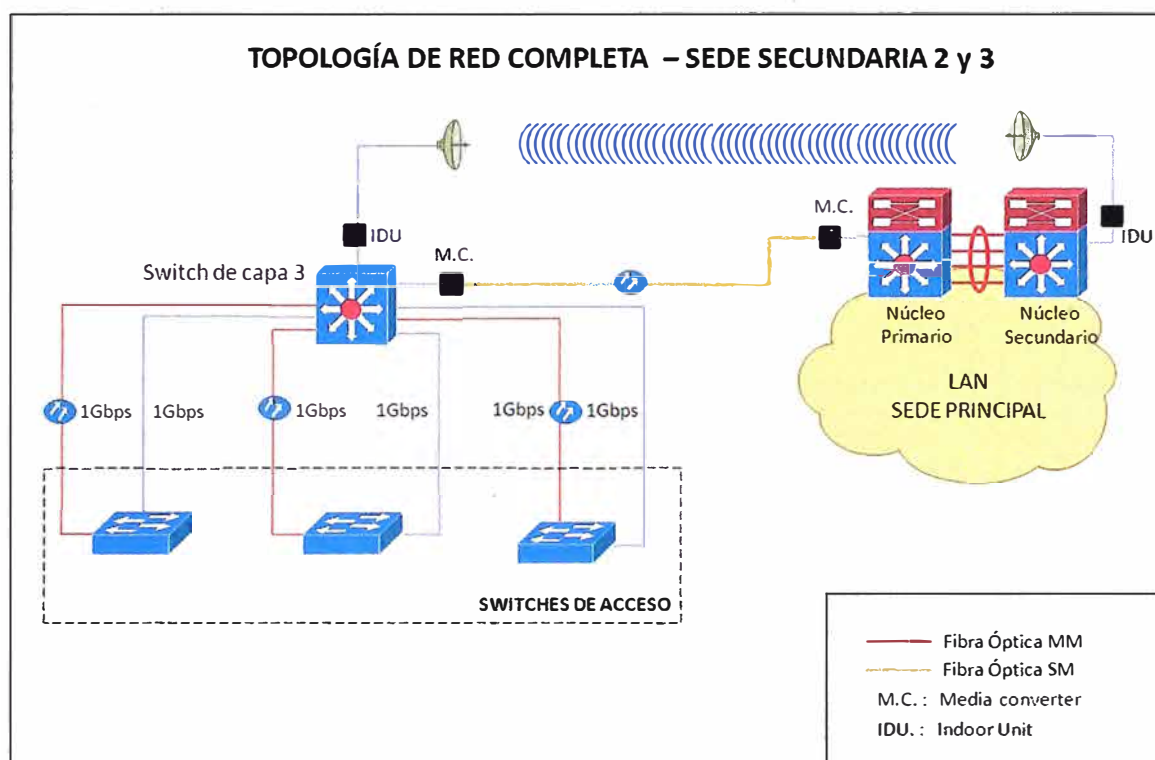


Figura 4.7 Topología de red completa – sede secundaria 2 y 3

En la tabla N°4.13 se muestran los requisitos mínimos que deben cumplir los switches de acceso de 48 puertos de las sedes secundarias 2 y 3.

En la tabla N°4.14 se muestran los requisitos mínimos que deben cumplir los switches de acceso de 24 puertos de las sedes secundarias 2 y 3.

En la tabla N°4.15 se muestran los requisitos mínimos que deben cumplir los switches de capa 3 de las sedes secundarias 2 y 3.

TABLA N° 4.13 Requisitos mín. de los switches acceso 48 pto. sede secundaria 2 y 3

Requisito	Switch de acceso
Cantidad de switches de acceso	4
Capacidad de conmutación mínima para switch de acceso	13.6 Gbps
Número de puertos de F.O. a 1 Gbps, multi-modo, de up-link	1
Número de puertos de RJ45 a 1 Gbps de up-link	1
Número de puertos RJ45, de 100 Mbps	48

TABLA N° 4.14 Requisitos min. de los switches acceso 24 ptos. sede secundaria 2 y 3

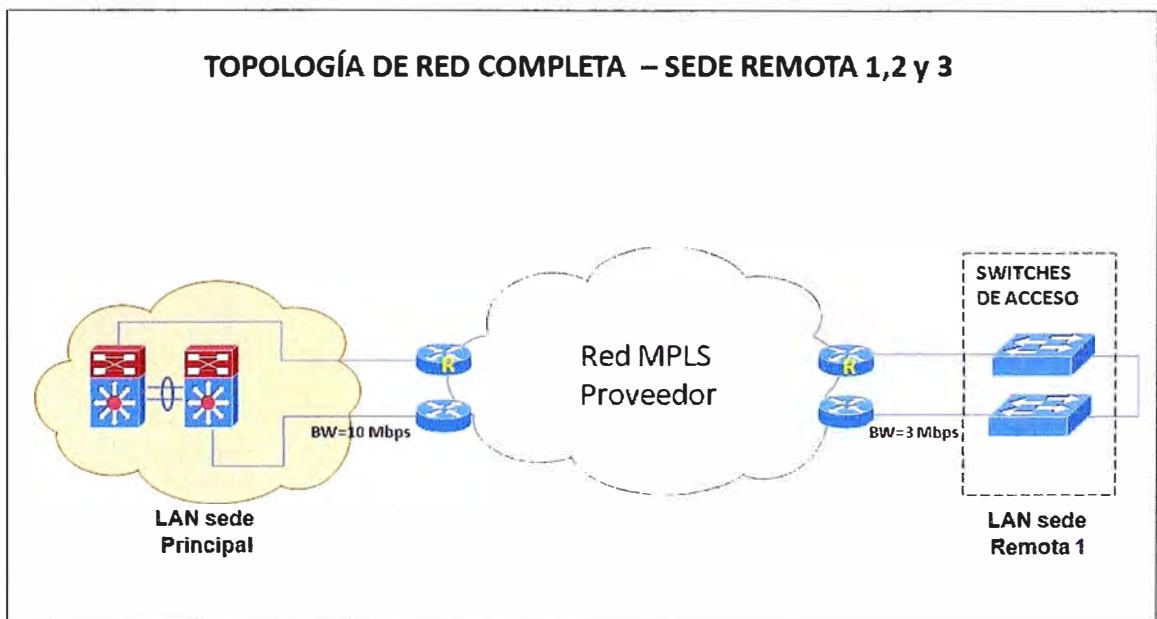
Requisito	Switch de acceso
Cantidad de switches de acceso	2
Capacidad de conmutación mínima para switch de acceso	8.8 Gbps
Número de puertos de F.O. a 1 Gbps, multi-modo, de up-link	1
Número de puertos de RJ45 a 1 Gbps de up-link	1
Número de puertos RJ45, de 100 Mbps	24

TABLA N° 4.15 Requisitos mínimos de los switches capa 3 sede secundaria 2 y 3

Requisito	Switch de capa 3
Cantidad de switches de capa 3	2
Capacidad de conmutación mínima para switch de acceso	16 Gbps
Número de puertos de F.O. a 1 Gbps, multi-modo, de up-link	4
Número de puertos RJ45, a 1 Gbps	24

• Cálculo de los requisitos - sedes remotas 1, 2 y 3

Las sedes remotas 1, 2 y 3 cuentan con la misma cantidad de switches en su implementación según la tabla N°4.10, en la figura 4.8 se muestra la topología de la red para estas sedes y su modo de conexión a la sede principal.



Las sede remotas 1, 2 y 3 no cuentan con un switch de capa 3, en su lugar la conexión con la sede principal se realiza a través de la red de transporte de un proveedor de

servicios de telecomunicaciones, igual que con el caso de las sedes secundarias el tráfico hacia la red principal es reducido, por lo cual consideraremos para todas las sedes remotas que los usuarios trabajaran a 100 Mbps.

En la tabla 4.16 se muestran los requisitos mínimos de los switches de acceso de las sedes remotas 1, 2 y 3 calculados en base a las ecuaciones (4.1) y (4.5)

TABLA N° 4.16 Requisitos mínimos de los switches acceso sede remota 1, 2 y 3

Requisito	Switch de acceso
Cantidad de switches de acceso	6
Capacidad de conmutación mínima para switch de acceso	13.6 Gbps
Número de puertos de RJ45 a 1 Gbps de up-link	2
Número de puertos RJ45, de 100 Mbps	48

•Cálculo de los requisitos - sedes remotas 4 y 5

Las sedes remotas 4 y 5 cuentan con la misma cantidad de switches en su implementación según la tabla N°4.10, en la figura 4.9 se muestra la topología de red para las sedes remotas 4 y 5, además se muestra el modo de conexión con la sede principal que es a través de la red de un proveedor de servicios de telecomunicaciones.

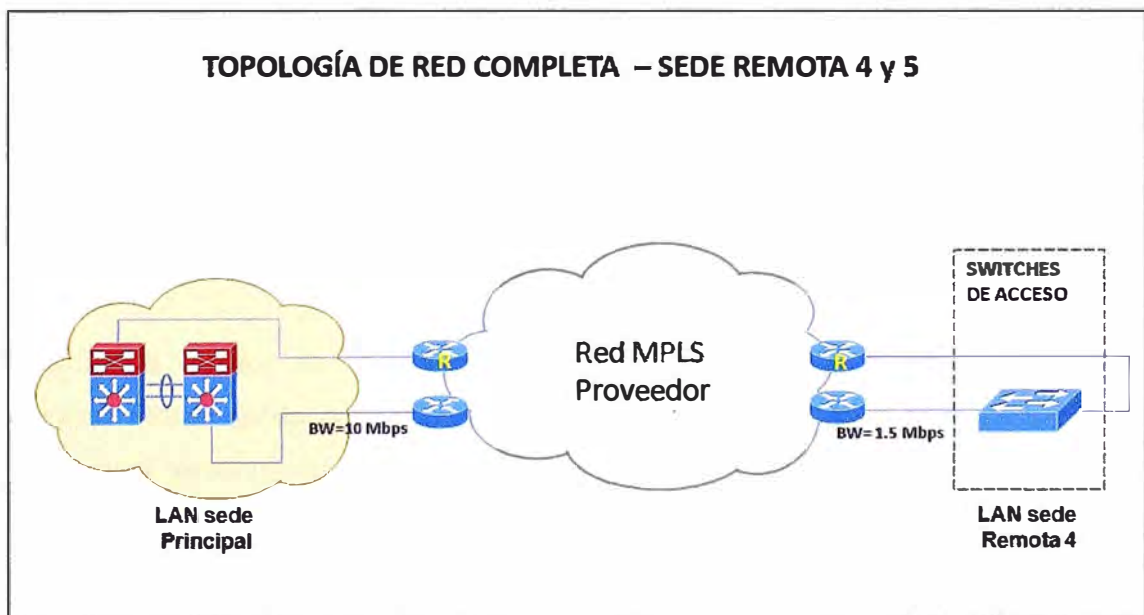


Figura 4.9 Topología de red completa – sede remota 4 y 5

En estas sedes solo se tiene implementado un switch de acceso de 48 puertos, en la tabla 4.17 se muestran los requisitos mínimos de los switches de acceso de las sedes remotas 4 y 5 calculados en base a las ecuaciones (4.1) y (4.5)

TABLA N° 4.17 Requisitos mínimos de los switches acceso sede remota 4 y 5

Requisito	Switch de acceso
Cantidad de switches de acceso	2
Capacidad de conmutación mínima para switch de acceso	13.6 Gbps
Número de puertos de RJ45 a 1 Gbps, multi-modo, de up-link	2
Número de puertos RJ45, de 100 Mbps	48

4.1.5 Detalle de diseño

Para dividir el gran dominio de broadcast de la toda la red corporativa en dominios de broadcast más pequeños usaremos el concepto de VLAN en el diseño de nuestra red, este concepto hará más eficiente el rendimiento de nuestra red ya que cada dominio de broadcast que se genera tendrá un número mucho menor de dispositivos, y el tráfico de estas VLAN no se mezclarán entre sí.

Las VLANs serán creadas para cada piso y se definirá una VLAN de datos y una de voz por piso, en el caso de las sedes secundarias y las sedes remotas se considerará una VLAN de datos y una de voz.

El direccionamiento IP para los datos será la siguiente red de clase B privada:

172.16.0.0 /12

Asimismo el direccionamiento IP para la voz será la siguiente red de clase A privada:

10.0.0.0 /8

Basados en la técnica de VLSM y en los datos de la tabla N°4.10, se realiza las operaciones matemáticas correspondientes a fin de tener el direccionamiento para las sedes principal, secundarias y remotas.

En la tabla N°4.18 se muestra el direccionamiento IP para la sede principal tanto para datos como para voz, asimismo se asigna un VLAN ID para cada VLAN creada.

En la tabla N°4.19 se muestra el direccionamiento IP para las sedes secundarias 1, 2 y 3 tanto para datos como para voz, asimismo se asigna un VLAN ID para cada VLAN creada.

En la tabla N°4.20 se muestra el direccionamiento IP para las sedes remotas 1, 2, 3, 4 y 5 tanto para datos como para voz, asimismo se asigna un VLAN ID para cada VLAN creada.

TABLA N° 4.18 Direccionamiento IP – Sede principal

SEDE PRINCIPAL						
Piso	Segmento de datos			Segmento de voz		
	VLAN ID	Segmento IP	Máscara	VLAN ID	Segmento IP	Máscara
1	20	172.16.208.0	255.255.255.0	40	10.20.48.0	255.255.255.0
2	21	172.16.209.0	255.255.255.0	41	10.20.49.0	255.255.255.0
3	22	172.16.210.0	255.255.255.0	42	10.20.50.0	255.255.255.0
4	23	172.16.211.0	255.255.255.0	43	10.20.51.0	255.255.255.0
5	24	172.16.212.0	255.255.255.0	44	10.20.52.0	255.255.255.0
6	25	172.16.213.0	255.255.255.0	45	10.20.53.0	255.255.255.0
7	26	172.16.214.0	255.255.255.0	46	10.20.54.0	255.255.255.0
8	27	172.16.215.0	255.255.255.0	47	10.20.55.0	255.255.255.0
9	28	172.16.216.0	255.255.255.0	48	10.20.56.0	255.255.255.0
10	29	172.16.217.0	255.255.255.0	49	10.20.57.0	255.255.255.0
11	30	172.16.218.0	255.255.255.0	50	10.20.58.0	255.255.255.0
12	31	172.16.219.0	255.255.255.0	51	10.20.59.0	255.255.255.0

TABLA N° 4.19 Direccionamiento IP – Sedes Secundarias

SEDE SECUNDARIA 1						
Piso	Segmento de datos			Segmento de voz		
	VLAN ID	Segmento IP	Máscara	VLAN ID	Segmento IP	Máscara
1, 2 y 3	15	172.16.226.0	255.255.252.0	22	10.20.30.0	255.255.252.0
SEDE SECUNDARIA 2						
Piso	Segmento de datos			Segmento de voz		
	VLAN ID	Segmento IP	Máscara	VLAN ID	Segmento IP	Máscara
1	2	172.16.249.0	255.255.255.0	3	10.20.60.0	255.255.255.0
SEDE SECUNDARIA 3						
Piso	Segmento de datos			Segmento de voz		
	VLAN ID	Segmento IP	Máscara	VLAN ID	Segmento IP	Máscara
1	2	172.16.254.0	255.255.255.0	3	10.20.254.0	255.255.255.0

TABLA N° 4.20 Direccionamiento IP – Sedes Remotas

SEDES REMOTAS						
Sede	Segmento de datos			Segmento de voz		
	VLAN ID	Segmento IP	Máscara	VLAN ID	Segmento IP	Máscara
remota 1	2	172.16.7.0	255.255.255.0	3	10.20.7.0	255.255.255.0
remota 2	2	172.16.8.0	255.255.255.0	3	10.20.8.0	255.255.255.0
remota 3	2	172.16.9.0	255.255.255.0	3	10.20.9.0	255.255.255.0
remota 4	2	172.16.10.0	255.255.255.0	3	10.20.10.0	255.255.255.0
remota 5	2	172.16.11.0	255.255.255.0	3	10.20.11.0	255.255.255.0

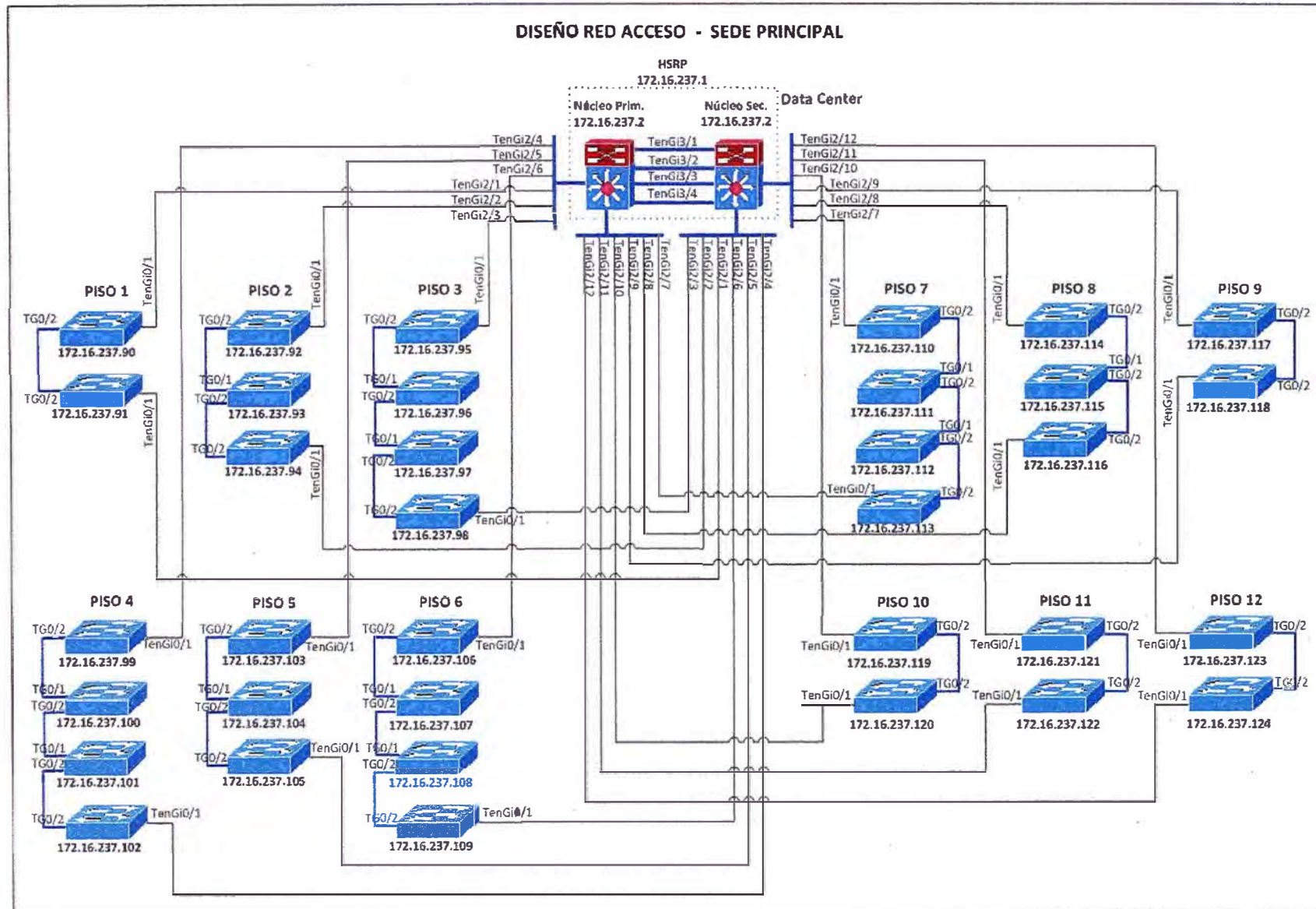


Figura 4.10 Diseño de red de acceso – sede principal

DISEÑO DE LA CONEXIÓN DE SEDES SECUNDARIAS CON LA SEDE PRINCIPAL

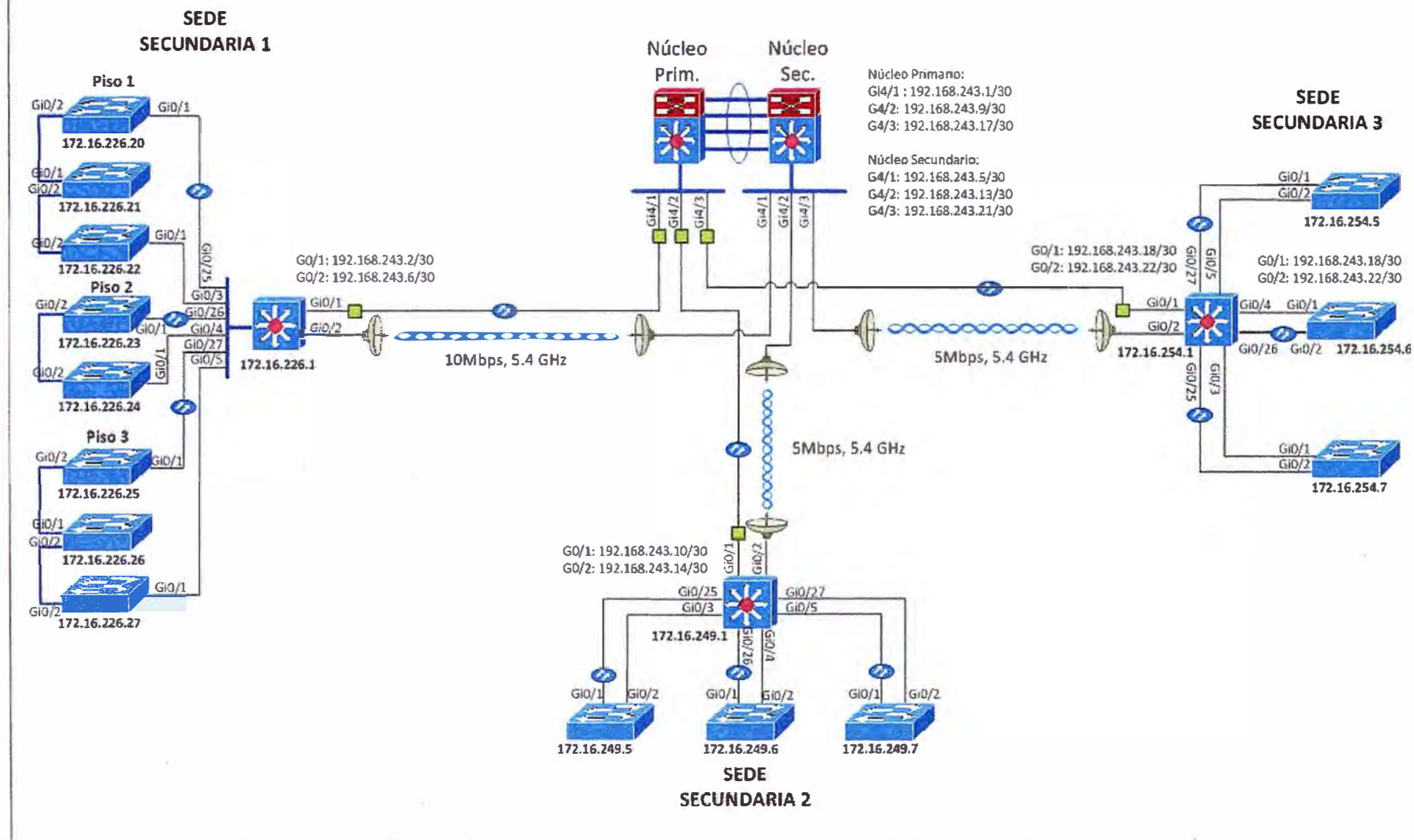


Figura 4.11 Diseño de la conexión de sedes secundarias con la sede principal

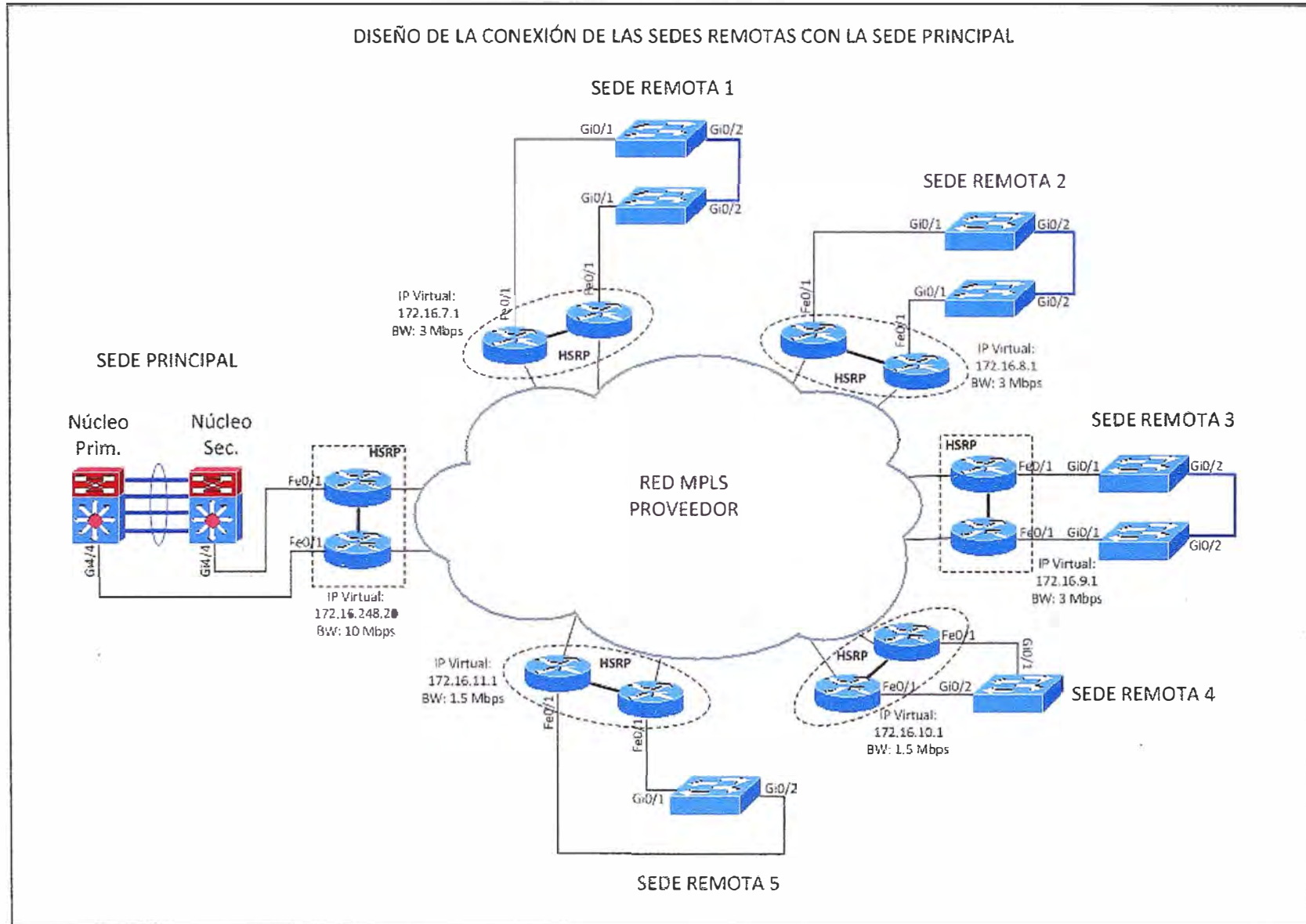


Figura 4.12 Diseño de la conexión de las sedes remotas con la sede principal

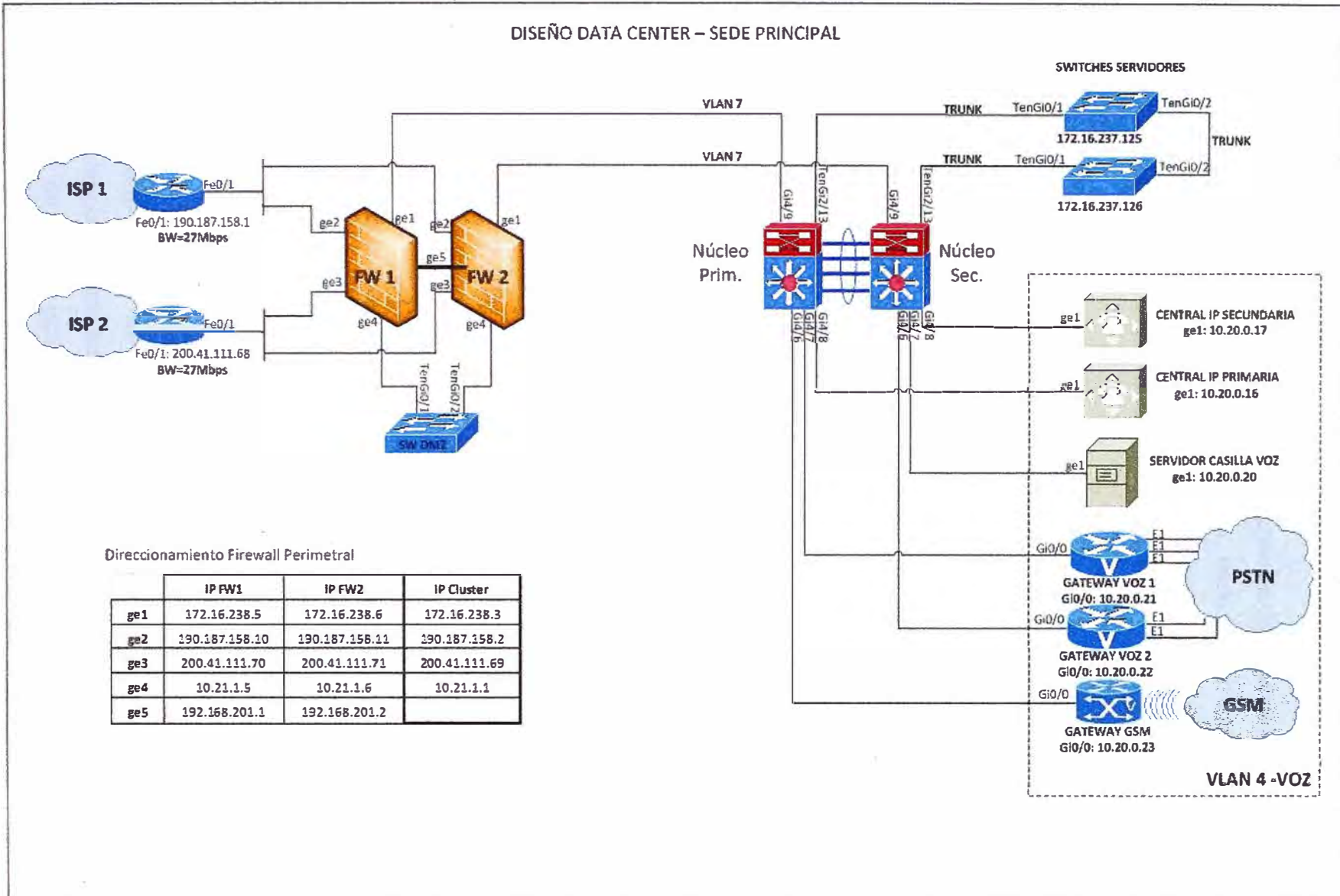


Figura 4.13 Diseño Data Center – Sede Principal

4.2. Dimensionamiento del proyecto

4.2.1. Dimensionamiento de los switches

Para realizar el dimensionamiento del proyecto tenemos que basarnos en la cantidad de equipos switches calculados en la sección anterior, dado que no todos los switches son iguales a pesar de que puedan tener la mismas cantidad de puertos o la misma velocidad por puerto, se debe definir los tipos de switches necesarios y la cantidad que se requieren de cada uno.

De acuerdo a la estructura de la red definida en la sección 4.1 tenemos los siguientes tipos de equipos:

- Switch tipo A – Definimos así al switch de Núcleo.
- Switch tipo B – Definimos así al switch de capa 3 que sirve para la conectividad de las sedes secundarias con la sede principal.
- Switch tipo C – Definimos así a los switches con las siguientes características de puertos:
 - ✓ Switch de acceso
 - ✓ 48 puertos RJ45 de 1Gbps
 - ✓ 2 puertos F.O. Up-link de 10 Gbps
- Switch tipo D – Definimos así a los switches con las siguientes características de puertos:
 - ✓ Switch de acceso
 - ✓ 48 puertos RJ45 de 100 Mbps
 - ✓ 1 puerto F.O. Up-link de 1 Gbps
 - ✓ 1 puerto RJ45 Up-link de 1 Gbps
- Switch tipo E - Definimos así a los switches con las siguientes características de puertos:
 - ✓ Switch de acceso
 - ✓ 24 puertos RJ45 de 100 Mbps
 - ✓ 2 puertos RJ45 Up-link de 1 Gbps

Se tiene calculado el total de switches por tipo que se necesita dentro de la red corporativa, se ha considerado tener un respaldo de equipos para que sean reemplazados en caso alguno de que un equipo en producción presente una falla, la estimación del respaldo es de aproximadamente 10 %, este respaldo no está considerado para los switches de núcleo.

En la tabla N°4.21 se muestra el total de equipos switches por tipo.

TABLA N° 4.21 Número de switches por tipo en la corporación

TIPO	Cantidad	Respaldo	Total
Switch tipo A	2	0	2
Switch tipo B	3	1	4
Switch tipo C	38	4	42
Switch tipo D	20	2	22
Switch tipo E	2	1	3

4.2.2. Dimensionamiento de la solución de telefonía IP

En la sección 3.2 se realizó el cálculo de la demanda, en base a la cantidad de usuarios y de teléfonos obtenida en ese proceso mostramos la contabilización de esta solución en la tabla N° 4.22.

TABLA N° 4.22 Dimensionamiento de la solución Telefonía IP

TIPO	Cantidad	Respaldo	Total
Teléfonos IP	1380	50	1430
Central Telefónica	2	0	2
Servidor mensajería	1	0	1
Router Gateway - 3 ptos. E1	2	0	2
Gateway GSM - 24 ptos.	1	0	1

4.2.3. Dimensionamiento de la seguridad perimetral

Como se indicó anteriormente la red corporativa contará con un arreglo de equipos en clúster a fin de brindar seguridad perimetral contra la red externa, la contabilización de equipos se muestra en la tabla N° 4.23.

TABLA N° 4.23 Dimensionamiento de los equipos de seguridad

TIPO	Cantidad	Respaldo	Total
Firewall Perimetral	2	0	2

De esta manera se contabilizó la cantidad de equipamiento necesario para la implementación de la red corporativa.

4.3. Especificaciones técnicas

A continuación indicamos las especificaciones técnicas que debe de cumplir el equipamiento a implementar.

4.3.1. Especificaciones técnicas de los switches

En la tabla N°4.24 se muestra las especificaciones técnicas de los diferentes tipos de switches que conforman la red corporativa.

TABLA N° 4.24 Especificaciones técnicas de los equipos switches en la red corporativa

SWITCH TIPO A	
Tipo de arquitectura	Modular
Número de slots mínimos	7
Capacidad de conmutación mínima	976 Gbps
Tarjeta tipo supervisora	Si
Número de puertos de F.O. a 10 Gbps, Multimodo como mínimo	28
Número de puertos RJ45, de 1Gbps	48
Tipo de redundancia	Activo - Activo
Soportar estándar 802.3af (PoE)	Si
Soporta estándar 802.1 d (STP)	Si
Soporta estándar 802.1 Q	Si
Soporta estándar 802.1 X	Si
Soporta estándar IEEE 802.3ad	Si
SWITCH TIPO B	
Capacidad de conmutación mínima	16 Gbps
Número de puertos de F.O. a 1 Gbps, multi-modo, de up-link	4
Número de puertos RJ45, a 1 Gbps	24
Soportar estándar 802.3af (PoE)	Si
Soporta estándar 802.1 d (STP)	Si
Soporta estándar 802.1 Q	Si
Soporta estándar 802.1 X	Si
Soporta estándar IEEE 802.3ad	Si
SWITCH TIPO C	
Capacidad de conmutación mínima	136 Gbps
Número de puertos de F.O. a 10 Gbps, multi-modo, de up-link	2
Número de puertos RJ45, de 1 Gbps	48
Soporta estándar 802.3af (PoE)	Si
Soporta estándar 802.1 d (STP)	Si
Soporta estándar 802.1 Q	Si
Soporta estándar 802.1 X	Si
Soporta estándar IEEE 802.3ad	Si
SWITCH TIPO D	
Capacidad de conmutación mínima para switch de acceso	13.6 Gbps
Número de puertos de F.O. a 1 Gbps, multi-modo, de up-link	1
Número de puertos de RJ45 a 1 Gbps, multi-modo, de up-link	1
Número de puertos RJ45, de 100 Mbps	48
Soporta estándar 802.3af (PoE)	Si
Soporta estándar 802.1 d (STP)	Si
Soporta estándar 802.1 Q	Si
Soporta estándar 802.1 X	Si
Soporta estándar IEEE 802.3ad	Si
SWITCH TIPO E	
Capacidad de conmutación mínima para switch de acceso	8.8 Gbps
Número de puertos de F.O. a 1 Gbps, multi-modo, de up-link	1

Número de puertos de RJ45 a 1 Gbps, multi-modo, de up-link	1
Número de puertos RJ45, de 100 Mbps	24
Soporta estándar 802.3af (PoE)	Si
Soporta estándar 802.1 d (STP)	Si
Soporta estándar 802.1 Q	Si
Soporta estándar 802.1 X	Si
Soporta estándar IEEE 802.3ad	Si

4.3.2. Especificaciones técnicas de los equipos de telefonía IP

En la tabla N°4.25 se muestran las especificaciones técnicas de la solución de telefonía IP que dará servicio a los usuarios de la corporación.

TABLA N° 4.25 Especificaciones técnicas de la solución de telefonía IP

Teléfono IP	
Velocidad de puerto RJ45	100/1000 Mbps
Número de puertos RJ45 a 100/1000 Mbps	2
Soportar H.323/ SIP	Si
Soportar estándar 802.3af (PoE)	Si
Soportar Códec G.711, G.729	Si
Soportar RTP, RTCP, cRTP	Si
Soporta estándar 802.1 Q	Si
Central Telefónica IP	
Número de puertos 100/1000 Ethernet como mínimo	1
Soportar H.323/SIP	Si
Número de suscritos como mínimo	1380
Soportar Códec G.711, G.729	Si
Soportar RSVP	Si
Soportar RTP, RTCP, cRTP	Si
Soporta estándar 802.1 X	Si
Tipo de redundancia	Activo - Activo
Soporta estándar 802.1 Q	Si
Servidor Mensajería de Voz	
Número de suscritos como mínimo	1380
Capacidad de almacenamiento casilla de voz como mínimo	10 Gbytes
Velocidad de puerto RJ45	100/1000 Mbps
Soporta estándar 802.1 X	Si
Soportar Códec G.711, G.729	Si
Tipo de redundancia	Activo - Activo
Router Gateway	
Velocidad de puerto RJ45	100/1000 Mbps
Número de puertos E1	3
Debe manejar 90 llamadas concurrentes como mínimo	Si
Soporta estándar 802.1 X	Si
Soporta estándar 802.1 Q	Si

Soportar G.711 PCM A-law/u-law	Si
Gateway GSM	
Velocidad de puerto RJ45	100/1000 Mbps
Debe manejar 18 llamadas concurrentes como mínimo	Si
Número de canales GSM como mínimo	18
Trabajar en las bandas GSM 850/900/1800/1900 MHz	Si
Soportar G.711 PCM A-law/u-law	Si

4.3.3. Especificaciones técnicas del equipo de seguridad perimetral

En la tabla N°4.26 se muestran las especificaciones técnicas de la solución de seguridad perimetral que brinda protección a toda la información y al equipamiento de telecomunicaciones de la red.

TABLA N° 4.26 Especificaciones técnicas de la solución de seguridad perimetral

Firewall Perimetral	
Capacidad de conmutación mínima	10Gbps
Número de puertos RJ45, de 1Gbps mínimo	5
Tipo de redundancia	Activo - Activo
Soporta estándar 802.1 Q	Si
Soporta estándar IEEE 802.3ad	Si

4.4. Subsistema de energía y protección eléctrica

El circuito eléctrico que brinda energía a nuestros equipos de telecomunicaciones lo hace también a otros equipos que brindan otros servicios, para este caso en particular consideraremos únicamente el subsistema de energía para el equipamiento de telecomunicaciones.

El subsistema de energía eléctrico cuenta con relés de protección ante cualquier problema que se pueda presentar, sin embargo al activarse estos relés, para el caso de los equipos de data center o de los switches de acceso, todo el equipamiento de telecomunicaciones se quedarían sin energía lo cual tendría un impacto negativo en la red y dejaría sin servicio a los usuarios.

Además de lo indicado, un corte o una repentina subida de la energía eléctrica podrían provocar problemas de funcionamiento en los equipos, especialmente de data center.

En la figura 4.14 se muestra el subsistema de energía eléctrico y los diferentes servicios que ofrece.

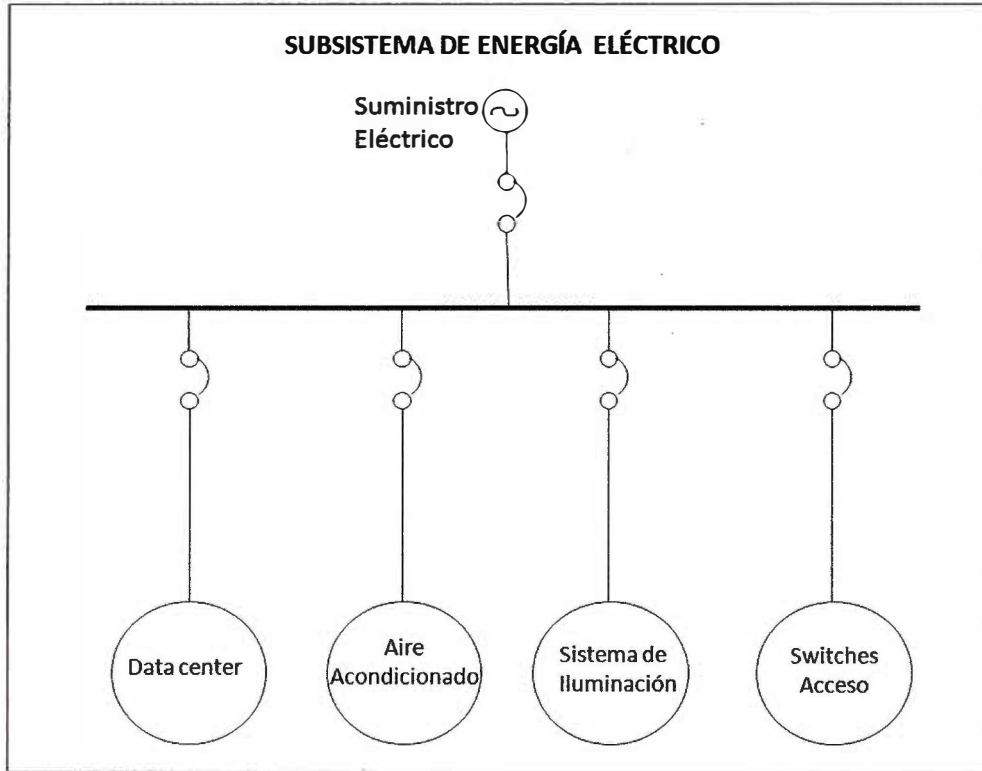


Figura 4.14 Subsistema de energía eléctrica

Una forma de evitar estos problemas es con la instalación de un equipo denominado UPS (Uninterruptible power supply) el cual, por lo general, consta de dos conexiones una conexión va al toma del suministro eléctrico y la otra alimenta a los equipos, en este caso de telecomunicaciones.

Los UPS cuentan también con baterías que permiten la continuidad del servicio incluso cuando la energía eléctrica comercial se ha suprimido.

A continuación vamos a calcular el valor de potencia requerido para cada una de las sedes en la corporación, para esto consideraremos los siguientes valores promedios indicados en la tabla N° 4.27.

TABLA N° 4.27 Potencias promedios

Tipo de equipo	Potencia promedio (KVA)
Switch de acceso	0,5
Switch de núcleo	5
Router	0,5
Servidores, firewall, etc.	0,5

En la tabla N°4.28 se calcula el valor de la potencia consumida en la sede principal.

TABLA N° 4.28 Potencia sede principal

Sede Principal			
Ubicación	N° equipos 48 puertos	N° equipos 24 puertos	Potencia KVA
Piso1	2	0	1
Piso2	3	0	1,5
Piso3	4	0	2
Piso4	4	0	2
Piso5	3	0	1,5
Piso6	4	0	2
Piso7	4	0	2
Piso8	3	0	1,5
Piso9	2	0	1
Piso10	2	0	1
Piso11	2	0	1
Piso12	2	0	1
Total			17,5

En la tabla N°4.29 se calcula el valor de la potencia consumida en la sede secundaria 1.

TABLA N° 4.29 Potencia sede secundaria 1

Sede Secundaria 1			
Ubicación	N° equipos 48 puertos	N° equipos 24 puertos	Potencia KVA
Piso1	3	0	1,5
Piso2	2	0	1
Piso3	3	0	1,5
Switch Capa 3	1	0	0,5
Total			4,5

En la tabla N°4.30 se calcula el valor de la potencia consumida en las sedes secundarias 2 y 3 y en las sedes remotas.

TABLA N° 4.30 Potencia sedes remotas

Sedes Remotas				
Ubicación	N° Equipos capa 3	N° equipos 48 puertos	N° equipos 24 puertos	Potencia KVA
Sede Secundaria 2	1	2	1	2
Sede Secundaria 3	1	2	1	2
Sede Remota 1	0	2	0	1
Sede Remota 2	0	2	0	1
Sede Remota 3	0	2	0	1
Sede Remota 4	0	1	0	0,5
Sede Remota 5	0	1	0	0,5

En el datacenter se encuentran los equipos más críticos de la red, la importancia de tener un sistema de UPS que proteja y brinde continuidad a estos equipos es muy alta, en la tabla N°4.31 se muestra la potencia consumida por los equipos de telecomunicaciones que se encuentran en el data center.

TABLA N° 4.31 Potencia data center

Equipos en datacenter	Cantidad	Potencia KVA
Switches de núcleo	2	10
Central telefónica	2	1
Router Gateway	2	1
Router GSM	1	0,5
Servidor de mensajería de voz	1	0,5
Switch DMZ	1	0,5
Sala de datos (P 7) – SW	2	1
Firewall Perimetral	2	1
Equipo de proveedores	10	5
Total		20,5

En la tabla N°4.32 se muestra las potencias consumidas en el datacenter y en cada una de las sedes de la corporación, en función de lo calculado se debe instalar un UPS.

TABLA N° 4.32 Potencias por sede

Ambientes en orden de prioridad	Potencia KVA
Equipos en data center	20,5
Sede principal	17,5
Sede secundaria 1	4,5
Sede Secundaria 2	2
Sede Secundaria 3	2
Sede Remota 1	1
Sede Remota 2	1
Sede Remota 3	1
Sede Remota 4	0,5
Sede Remota 5	0,5

En nuestro caso consideramos prioritario dar protección y continuidad a los equipos que están en el data center.

Continuando con el orden de prioridad se instala un UPS para dar protección y continuidad de servicio a los switches de acceso en la sede principal, de la misma manera se tiene el valor de carga de las UPS para las demás sedes a fin de que también sean instalados.

En la figura 4.15 se muestra el modo en el que se debe instalar los UPS.

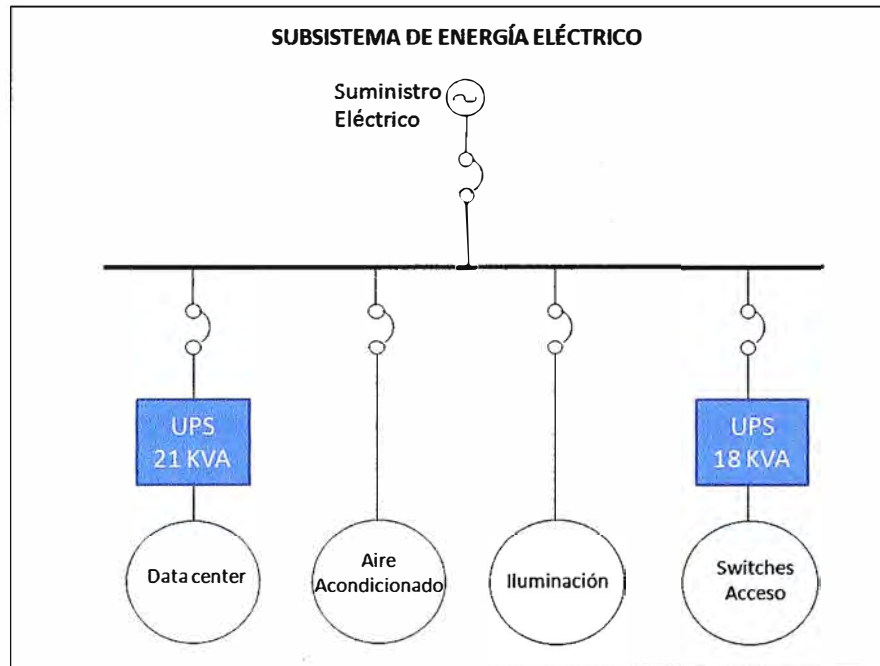


Figura 4.15 Subsistema de energía eléctrica

Con respecto a la protección eléctrica, se indicó previamente que los UPS tienen como una de sus funciones proteger a los equipos, en este caso de telecomunicaciones, ante los cambios bruscos del voltaje comercial, la otra función es la de brindar continuidad de servicio en caso de corte de energía.

Otra manera de protección eléctrica es mediante el sistema de puesta a tierra. La puesta a tierra se emplea en las instalaciones eléctricas para evitar el paso de corriente al usuario por un fallo del aislamiento de los conductores activos. Asimismo protege a los equipos de posibles corrientes de pico que se puedan generar.

El sistema de puesta a tierra cuenta con un pozo a tierra el cual presenta una impedancia baja (menos de 5 ohmios), el cual lleva una conexión hacia los chasis de los equipos de comunicaciones.

Con el pozo a tierra a poca impedancia se busca que toda corriente de fuga o estática siempre pase a través de la conexión a tierra y de esta manera se protege no solo a la persona que es lo más importante sino también a los equipos que tenemos conectados a tierra.

CAPÍTULO V COSTO DEL PROYECTO

5.1. Costos de inversión de implementación

5.1.1. Costo por compra equipos propios

En la tabla N°5.1 se muestra el precio unitario del equipamiento de telecomunicaciones que incluye la garantía del fabricante por 2 años, además del servicio de soporte y mantenimiento del fabricante también por 2 años, los precios están expresados en USD.

TABLA N° 5.1 Precio del equipamiento de telecomunicaciones

EQUIPOS SWITCHES	PRECIO UNITARIO	CANTIDAD	Valor total (USD)
Switch tipo A	40000	2	80000
Switch tipo B	4500	4	18000
Switch tipo C	5000	42	210000
Switch tipo D	5000	22	110000
Switch tipo E	3000	3	9000
EQUIPOS DE TELEFONIA IP	PRECIO UNITARIO	CANTIDAD	Valor total
Teléfonos IP	250	1430	357500
Central Telefónica	30000	2	60000
Servidor mensajería	30000	1	30000
Router Gateway - 3 ptos. E1	3000	2	6000
Gateway GSM - 24 ptos.	2000	1	2000
EQUIPOS DE SEGURIDAD	PRECIO UNITARIO	CANTIDAD	Valor total
Firewall Perimetral	8000	2	16000
EQUIPOS DE RADIO ENLACE	PRECIO UNITARIO	CANTIDAD	Valor total
Radio enlaces @ 5MHz	800	6	4800
Sub Total (USD)			903300

5.1.2. Costo por instalación y configuración de equipos propios

En la tabla N° 5.2 se muestra el precio por concepto de instalación y configuración del equipamiento de telecomunicaciones, el cual será realizado por el personal de una empresa especialista en el rubro.

TABLA N° 5.2 Precio del servicio de instalación y configuración

SERVICIO PROFESIONAL	N° de horas	Costo x hora (USD)	Valor total (USD)
Implementación de la solución switches	80	70	5600
Implementación de la solución telefonía	50	70	3500
Implementación de la solución seguridad	15	70	1050
Implementación de enlaces de radio	50	70	3500
Sub Total (USD)			13650

Fuente: Elaboración propia

5.1.3. Costo por instalación de servicios arrendados

En la tabla N° 5.3 se muestra el precio por concepto de la instalación de los equipos de los proveedores de servicios de telecomunicaciones a los cuales se arrienda servicios, estos trabajos de instalación generalmente implican la permanencia de equipos ajenos dentro de las instalaciones de la empresa.

TABLA N° 5.3 Precio de instalación de servicios arrendados

SERVICIO CONTRATADO	COSTO DE INSTALACIÓN	N° de servicios	Valor total (USD)
Servicio de Internet 27 Mbps ISP 1	1000	1	1000
Servicio de Internet 27 Mbps ISP 2	700	1	700
Servicio telefonía 5 Primarios	1000	1	1000
Instalación fibra Óptica oscura	500	6	3000
Instalación de acceso a red MPLS	500	6	3000
Sub Total (USD)			8700

Fuente: Elaboración propia

Finalmente el costo de inversión de implementación (CII) será igual a:

$$CII = 903300 + 13650 + 8700 = 925,650.00 \text{ USD}$$

(5.1)

5.2. Costos de operación y mantenimiento

5.2.1. Costos de operación

• Costo del personal encargado

A fin de evitar gastos administrativos a la empresa y dado la envergadura de la red, se considera como mejor opción contratar a una empresa outsourcing especializada en la administración y gestión de servicios de telecomunicaciones.

El costo del personal de mantenimiento vendrá dado por los siguientes factores:

- Costo de operación en horario de oficina

En la tabla N° 5.4 se muestra el costo por concepto del servicio de administración y gestión de la red de telecomunicaciones en horario de oficina, se está considerando en el cálculo que se requerirán de dos especialistas para estas funciones.

TABLA N° 5.4 Costo de operación en horario de oficina

Costo x hora (USD)	Número de horas diarias	Número de días hábiles al mes	Número de especialistas	Costo mensual del servicio en horario de oficina (USD)
50	8	22	2	17600

Fuente: Elaboración propia

- Costo por concepto de disponibilidad en horario fuera de oficina

Debido a que la red de telecomunicaciones brinda servicios de manera continua a los usuarios es importante contar con personal disponible en horario fuera de oficina. En la tabla N°5.5 se muestra el costo en horario fuera de oficina por concepto de disponibilidad, para días hábiles es el 15% del costo por hora y el 30% del costo por hora en fines de semana, el cálculo es realizado considerando que solo una persona está disponible en horario fuera de oficina.

TABLA N° 5.5 Costo del servicio de disponibilidad en horario fuera de oficina

Días de semana				Fines de semana				TOTAL (USD)
Costo x hora (USD)	Horas x día	Nº de días	Total (USD)	Costo x hora (USD)	Horas x día	Nº de días	Total (USD)	
7,5	16	22	2640	15	24	8	2880	5520

Fuente: Elaboración propia

- Costo de atención de incidentes en horario fuera de oficina.

El costo de atención de incidentes en horario fuera de oficina lo estimaremos como el 10% de la suma del costo en horario de oficina y el costo del servicio de disponibilidad en horario fuera de oficina.

$$= 10\% \times (17600 + 5520) = 2,312.00 \text{ USD} \quad (5.2)$$

Finalmente el costo por concepto del personal encargado será la suma de los valores calculados anteriormente:

$$= 17600 + 5520 + 2312 = 25,432.00 \text{ USD} \quad (5.3)$$

• **Costo por concepto de servicios arrendados**

En la tabla N° 5.6 se muestra el costo mensual por el concepto de servicios de telecomunicaciones contratados a diferentes proveedores.

TABLA N° 5.6 Costo por servicios contratados

SERVICIO CONTRATADO	Costo mensual (USD)
Servicio de Internet 27 Megas ISP 1	1000
Servicio de Internet 27 Megas ISP 2	500
Servicio telefonía 5 Primarios	1000
Servicio de conectividad por fibra Óptica oscura (3 fibras oscuras S.M.)	1200
Servicio de conectividad por la red MPSSL (6 enlaces)	2400
Total (USD)	6100

Por lo tanto el costo por operación será:

$$\text{Costo por operación Mensual} = 25432 + 6100 = 31,532.00 \text{ USD} \quad (5.4)$$

5.2.2 Costo por mantenimiento de equipos propios

El precio de los equipos propios incluyen el servicio de soporte y mantenimiento por el lapso de dos años, estos no generarán gasto adicional por mantenimiento en ese lapso, luego de ese tiempo se debe optar por la revalidación del contrato de soporte con la marca, en la tabla 5.7 se muestra el costo por este concepto.

TABLA N° 5.7 Costo del mantenimiento en dos años

EQUIPOS PROPIOS	PRECIO UNITARIO X CONCEPTO DE SOPORTE, GARANTÍA Y MANTENIMIENTO	CANTIDAD	Valor total (USD)
Switch tipo A	5000	2	10000
Switch tipo B	800	4	3200
Switch tipo C	800	42	33600
Switch tipo D	800	22	17600
Switch tipo E	800	3	2400
Teléfonos IP	20	1430	28600
Central Telefónica	1000	2	2000
Servidor mensajería	1000	1	1000
Router Gateway - 3 ptos. E1	800	2	1600
Gateway GSM - 24 ptos.	600	1	600
Firewall Perimetral	1000	2	2000
Radio enlaces @ 5MHz	80	6	480
TOTAL (USD)			103080

Al paso de dos años el costo para renovar el servicio de soporte y mantenimiento de los equipos por dos años más es igual a **103,080.00 USD**.

Resumimos el valor de los costos para el proyecto en la tabla 5.8.

TABLA N° 5.8 Costos del proyecto

Costo de inversión de implementación	925,6500.00 USD
Costo por operación mensual	31,532.00 USD
Costo para renovar soporte y mantenimiento de equipos luego de 2 años	103,080.00 USD

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Los usuarios de la empresa cada vez demandan mayor ancho de banda para los servicios de telecomunicaciones lo cual sumando al ritmo del negocio implica un alto crecimiento de la demanda en un tiempo corto.
2. En el informe se muestra que la alta disponibilidad es un aspecto que se puede considerar en toda parte del diseño, en nuestro caso la red es altamente redundante en funcionamiento y brinda alta disponibilidad de servicios de telecomunicaciones.
3. Dimensionar las necesidades en base a proyecciones futuras nos ayuda a desarrollar una red de telecomunicaciones más escalable, de esta manera cada nuevo usuario que ingresa a la red tiene la misma capacidad que los usuarios anteriores sin afectar su desempeño.
4. Una alta disponibilidad de los servicios de red conlleva a una redundancia de los equipos de comunicaciones, el presente informe verifica que mientras más alta sea la disponibilidad de nuestros servicios los costos de implementación y operación relacionados también se incrementarán.

Recomendaciones

1. La empresa objeto de este estudio tiene la capacidad de asumir el costo de una red con redundancia a todo nivel dado lo crítico de sus operaciones, sin embargo para casos donde la empresa no maneje información crítica o no requiera de una disponibilidad tan alta se pueden obviar algunas de las consideraciones tomadas en el presente informe, lo cual no indica que la red ya no sea redundante sino que el nivel de redundancia será menor.
2. La demanda de servicios de telecomunicaciones va en constante aumento debido a varios factores, uno de estos factores es el crecimiento de usuarios en poco tiempo, por tal motivo las redes de acceso deben contar con servicios de autenticación y protección a fin de evitar potenciales ataques o problemas los servicios de la red.

3. Se debe restringir los accesos entre sedes que no sean necesarios, especialmente entre las sedes secundarias y remotas con la sede principal ya que hay muchos servicios localizados en la sede principal que solo son de utilidad para los usuarios de esta sede, por lo cual el hecho de restringir este tráfico ayuda a mantener un buen desempeño de la red.
4. En ventanas de mantenimiento establecidas cada cierto tiempo se debe realizar pruebas con los equipos dentro de la red de telecomunicaciones, para verificar que los equipos de comunicaciones trabajan de manera redundante como indica el diseño, se debe tener mucho cuidado en caso de realizar esto una vez que se tiene la red en producción.

GLOSARIO DE TÉRMINOS

- Ancho de banda: Cantidad de datos que se pueden transmitir en una unidad de tiempo.
- Backbone: Cableado troncal o subsistema vertical en una instalación de red de área local que sigue la normativa de cableado estructurado.
- Best-effort: Bajo este mecanismo, la red trata por igual a todos los paquetes de datos, sin dar prioridad a ningún tipo de tráfico sobre otro.
- Broadcast: Transmisión de datos que serán recibidos por todos los dispositivos en una red. Envía información a todos los dispositivos que se encuentren conectados en la misma red.
- CAR: Committed access rate, tasa de acceso contratada, es una métrica usada para acuerdos de calidad de servicio de internet para clasificar y limitar el tráfico del cliente y manejar exceso de tráfico de acuerdo con la política de la red.
- CIR: Committed Information Rate, tasa de información contratada, usado en redes Frame Relay es el ancho de banda promedio de un circuito digital garantizado por un proveedor de servicio de internet.
- Conmutación: Conexión que realizan los diferentes nodos que existen en distintos lugares para lograr conectar a dos usuarios de una red de telecomunicaciones.
- CRC: Cyclic redundancy check, comprobación de redundancia cíclica, es una técnica de detección de errores.
- CSMA /CD: Acceso múltiple con detección de portadora y detección de colisiones, es un método de control de acceso al medio usado sobre todo en las redes de área local que usaban tecnología Ethernet.
- Datagrama: Agrupamiento lógico de información enviado como una unidad de capa de red a través de un medio de transmisión sin establecer previamente un circuito virtual.
- Equipo de capa 3: Dispositivo de la capa de red del modelo OSI que utiliza una o más métricas para determinar la ruta óptima por la que se debe enviar el tráfico de la red.
- Erlang: Es una unidad adimensional utilizada en telefonía como una medida estadística del volumen de tráfico.
- Ethernet: Tecnología de red de área local que usaba una topología de bus.
- Firewall: Aplicación o dispositivo diseñado para prevenir comunicaciones no deseadas y no autorizadas entre redes de computadoras.

- Gateway GSM: Equipo que permite comunicar una red, como Ethernet con una la red celular de tecnología GMS.
- IEEE 802.3: Protocolo de LAN de IEEE que especifica una implementación de la capa física y la subcapa MAC de la capa de enlace de datos. IEEE 802.3 utiliza el acceso CSMA/CD a una serie de velocidades a través de diversos medios físicos.
- ISP: Internet Service Provider, Proveedor de Servicios de Internet, una compañía que proporciona acceso a Internet.
- Jitter: Es la variabilidad del tiempo de ejecución de los paquetes. Este efecto es especialmente molesto en aplicaciones multimedia en Internet como radio por Internet o telefonía IP, ya que provoca que algunos paquetes lleguen demasiado pronto o tarde para poder entregarlos a tiempo.
- Latencia: Es el tiempo transcurrido entre que un dispositivo recibe una trama y la reenvía al puerto destino.
- Línea primaria E1: Servicio de 30 líneas telefónicas digitales para las comunicaciones.
- Mensajes BPDU: Paquete hello del protocolo de árbol de extensión que se envía a intervalos que se pueden configurar para intercambiar información entre los puentes de la red.
- Multicast: Es un servicio de red en el cual un único flujo de datos, proveniente de una determinada fuente, puede ser enviada simultáneamente a un grupo de destinatarios.
- QoS: Quality of Service, calidad de servicio, es el rendimiento promedio de una red de telefonía o de computadoras, particularmente el rendimiento visto por los usuarios de la red. Para cuantitativamente medir la calidad de servicio son considerados varios aspectos del servicio de red, tales como tasas de errores, ancho de banda, rendimiento, retraso en la transmisión, disponibilidad, etc.
- Topología: Forma en que está diseñada la red, sea en el plano físico o lógico.
- Unicast: Envío de información desde un único emisor a un único receptor.
- Up-link: Es el medio de conexión entre dos lugares con el propósito de transmitir y recibir información
- UTP: Unshielded twisted pair, par trenzado sin blindaje, son cables de pares trenzados sin blindar que se utilizan para diferentes tecnologías de redes locales.

ANEXO A

Erlang B (Blocked Calls Cleared)

No. of Trunks (N)	Traffic (A) in erlangs																
	0.1%	0.2%	0.5%	1%	1.2%	1.3%	1.5%	2%	3%	5%	7%	10%	15%	20%	30%	40%	50%
1	0.001	0.002	0.005	0.010	0.012	0.013	0.02	0.020	0.031	0.053	0.075	0.111	0.176	0.250	0.429	0.667	1.00
2	0.046	0.065	0.105	0.153	0.168	0.176	0.19	0.223	0.282	0.381	0.470	0.595	0.796	1.00	1.45	2.00	2.73
3	0.194	0.249	0.349	0.455	0.489	0.505	0.53	0.602	0.715	0.899	1.06	1.27	1.60	1.93	2.63	3.48	4.59
4	0.439	0.535	0.701	0.869	0.922	0.946	0.99	1.09	1.26	1.52	1.75	2.05	2.50	2.95	3.89	5.02	6.50
5	0.762	0.900	1.13	1.36	1.43	1.46	1.52	1.66	1.88	2.22	2.50	2.88	3.45	4.01	5.19	6.60	8.44
6	1.15	1.33	1.62	1.91	2.00	2.04	2.11	2.28	2.54	2.96	3.30	3.76	4.44	5.11	6.51	8.19	10.4
7	1.58	1.80	2.16	2.50	2.60	2.65	2.73	2.94	3.25	3.74	4.14	4.67	5.46	6.23	7.86	9.80	12.4
8	2.05	2.31	2.73	3.13	3.25	3.30	3.40	3.63	3.99	4.54	5.00	5.60	6.50	7.37	9.21	11.4	14.3
9	2.56	2.85	3.33	3.78	3.92	3.98	4.08	4.34	4.75	5.37	5.88	6.55	7.55	8.52	10.6	13.0	16.3
10	3.09	3.43	3.96	4.46	4.61	4.68	4.80	5.08	5.53	6.22	6.78	7.51	8.62	9.68	12.0	14.7	18.3
11	3.65	4.02	4.61	5.16	5.32	5.40	5.53	5.84	6.33	7.08	7.69	8.49	9.69	10.9	13.3	16.3	20.3
12	4.23	4.64	5.28	5.88	6.05	6.14	6.27	6.61	7.14	7.95	8.61	9.47	10.8	12.0	14.7	18.0	22.2
13	4.83	5.27	5.96	6.61	6.80	6.89	7.03	7.40	7.97	8.83	9.54	10.5	11.9	13.2	16.1	19.6	24.2
14	5.45	5.92	6.66	7.35	7.56	7.65	7.81	8.20	8.80	9.73	10.5	11.5	13.0	14.4	17.5	21.2	26.2
15	6.08	6.58	7.38	8.11	8.33	8.43	8.59	9.01	9.65	10.6	11.4	12.5	14.1	15.6	18.9	22.9	28.2
16	6.72	7.26	8.10	8.88	9.11	9.21	9.39	9.83	10.5	11.5	12.4	13.5	15.2	16.8	20.3	24.5	30.2
17	7.38	7.95	8.83	9.65	9.89	10.0	10.19	10.7	11.4	12.5	13.4	14.5	16.3	18.0	21.7	26.2	32.2
18	8.05	8.64	9.58	10.4	10.7	10.8	11.00	11.5	12.2	13.4	14.3	15.5	17.4	19.2	23.1	27.8	34.2
19	8.72	9.35	10.3	11.2	11.5	11.6	11.82	12.3	13.1	14.3	15.3	16.6	18.5	20.4	24.5	29.5	36.2
20	9.41	10.1	11.1	12.0	12.3	12.4	12.65	13.2	14.0	15.2	16.3	17.6	19.6	21.6	25.9	31.2	38.2
21	10.1	10.8	11.9	12.8	13.1	13.3	13.48	14.0	14.9	16.2	17.3	18.7	20.8	22.8	27.3	32.8	40.2
22	10.8	11.5	12.6	13.7	14.0	14.1	14.32	14.9	15.8	17.1	18.2	19.7	21.9	24.1	28.7	34.5	42.1
23	11.5	12.3	13.4	14.5	14.8	14.9	15.16	15.8	16.7	18.1	19.2	20.7	23.0	25.3	30.1	36.1	44.1
24	12.2	13.0	14.2	15.3	15.6	15.8	16.01	16.6	17.6	19.0	20.2	21.8	24.2	26.5	31.6	37.8	46.1
25	13.0	13.8	15.0	16.1	16.5	16.6	16.87	17.5	18.5	20.0	21.2	22.8	25.3	27.7	33.0	39.4	48.1
26	13.7	14.5	15.8	17.0	17.3	17.5	17.72	18.4	19.4	20.9	22.2	23.9	26.4	28.9	34.4	41.1	50.1
27	14.4	15.3	16.6	17.8	18.2	18.3	18.59	19.3	20.3	21.9	23.2	24.9	27.6	30.2	35.8	42.8	52.1
28	15.2	16.1	17.4	18.6	19.0	19.2	19.45	20.2	21.2	22.9	24.2	26.0	28.7	31.4	37.2	44.4	54.1
29	15.9	16.8	18.2	19.5	19.9	20.0	20.32	21.0	22.1	23.8	25.2	27.1	29.9	32.6	38.6	46.1	56.1
30	16.7	17.6	19.0	20.3	20.7	20.9	21.19	21.9	23.1	24.8	26.2	28.1	31.0	33.8	40.0	47.7	58.1
31	17.4	18.4	19.9	21.2	21.6	21.8	22.07	22.8	24.0	25.8	27.2	29.2	32.1	35.1	41.5	49.4	60.1
32	18.2	19.2	20.7	22.0	22.5	22.6	22.95	23.7	24.9	26.7	28.2	30.2	33.3	36.3	42.9	51.1	62.1
33	19.0	20.0	21.5	22.9	23.3	23.5	23.83	24.6	25.8	27.7	29.3	31.3	34.4	37.5	44.3	52.7	64.1
34	19.7	20.8	22.3	23.8	24.2	24.4	24.72	25.5	26.8	28.7	30.3	32.4	35.6	38.8	45.7	54.4	66.1
35	20.5	21.6	23.2	24.6	25.1	25.3	25.60	26.4	27.7	29.7	31.3	33.4	36.7	40.0	47.1	56.0	68.1
36	21.3	22.4	24.0	25.5	26.0	26.2	26.49	27.3	28.6	30.7	32.3	34.5	37.9	41.2	48.6	57.7	70.1
37	22.1	23.2	24.8	26.4	26.8	27.0	27.39	28.3	29.6	31.6	33.3	35.6	39.0	42.4	50.0	59.4	72.1
38	22.9	24.0	25.7	27.3	27.7	27.9	28.28	29.2	30.5	32.6	34.4	36.6	40.2	43.7	51.4	61.0	74.1
39	23.7	24.8	26.5	28.1	28.6	28.8	29.18	30.1	31.5	33.6	35.4	37.7	41.3	44.9	52.8	62.7	76.1

40	24.4	25.6	27.4	29.0	29.5	29.7	30.08	31.0	32.4	34.6	36.4	38.8	42.5	46.1	54.2	64.4	78.1
41	25.2	26.4	28.2	29.9	30.4	30.6	30.98	31.9	33.4	35.6	37.4	39.9	43.6	47.4	55.7	66.0	80.1
42	26.0	27.2	29.1	30.8	31.3	31.5	31.88	32.8	34.3	36.6	38.4	40.9	44.8	48.6	57.1	67.7	82.1
43	26.8	28.1	29.9	31.7	32.2	32.4	32.79	33.8	35.3	37.6	39.5	42.0	45.9	49.9	58.5	69.3	84.1
44	27.6	28.9	30.8	32.5	33.1	33.3	33.69	34.7	36.2	38.6	40.5	43.1	47.1	51.1	59.9	71.0	86.1
45	28.4	29.7	31.7	33.4	34.0	34.2	34.60	35.6	37.2	39.6	41.5	44.2	48.2	52.3	61.3	72.7	88.1
46	29.3	30.5	32.5	34.3	34.9	35.1	35.51	36.5	38.1	40.5	42.6	45.2	49.4	53.6	62.8	74.3	90.1
47	30.1	31.4	33.4	35.2	35.8	36.0	36.42	37.5	39.1	41.5	43.6	46.3	50.6	54.8	64.2	76.0	92.1
48	30.9	32.2	34.2	36.1	36.7	36.9	37.34	38.4	40.0	42.5	44.6	47.4	51.7	56.0	65.6	77.7	94.1
49	31.7	33.0	35.1	37.0	37.6	37.8	38.25	39.3	41.0	43.5	45.7	48.5	52.9	57.3	67.0	79.3	96.1
50	32.5	33.9	36.0	37.9	38.5	38.7	39.17	40.3	41.9	44.5	46.7	49.6	54.0	58.5	68.5	81.0	98.1
51	33.3	34.7	36.9	38.8	39.4	39.6	40.08	41.2	42.9	45.5	47.7	50.6	55.2	59.7	69.9	82.7	100.1
52	34.2	35.6	37.7	39.7	40.3	40.6	41.00	42.1	43.9	46.5	48.8	51.7	56.3	61.0	71.3	84.3	102.1
53	35.0	36.4	38.6	40.6	41.2	41.5	41.92	43.1	44.8	47.5	49.8	52.8	57.5	62.2	72.7	86.0	104.1
54	35.8	37.2	39.5	41.5	42.1	42.4	42.84	44.0	45.8	48.5	50.8	53.9	58.7	63.5	74.2	87.6	106.1
55	36.6	38.1	40.4	42.4	43.0	43.3	43.77	44.9	46.7	49.5	51.9	55.0	59.8	64.7	75.6	89.3	108.1
56	37.5	38.9	41.2	43.3	43.9	44.2	44.69	45.9	47.7	50.5	52.9	56.1	61.0	65.9	77.0	91.0	110.1
57	38.3	39.8	42.1	44.2	44.8	45.1	45.62	46.8	48.7	51.5	53.9	57.1	62.1	67.2	78.4	92.6	112.1
58	39.1	40.6	43.0	45.1	45.8	46.1	46.54	47.8	49.6	52.6	55.0	58.2	63.3	68.4	79.8	94.3	114.1
59	40.0	41.5	43.9	46.0	46.7	47.0	47.47	48.7	50.6	53.6	56.0	59.3	64.5	69.7	81.3	96.0	116.1
60	40.8	42.4	44.8	46.9	47.6	47.9	48.40	49.6	51.6	54.6	57.1	60.4	65.6	70.9	82.7	97.6	118.1
61	41.6	43.2	45.6	47.9	48.5	48.8	49.33	50.6	52.5	55.6	58.1	61.5	66.8	72.1	84.1	99.3	120.1
62	42.5	44.1	46.5	48.8	49.4	49.7	50.26	51.5	53.5	56.6	59.1	62.6	68.0	73.4	85.5	101.0	122.1
63	43.3	44.9	47.4	49.7	50.4	50.7	51.19	52.5	54.5	57.6	60.2	63.7	69.1	74.6	87.0	102.6	124.1
64	44.2	45.8	48.3	50.6	51.3	51.6	52.12	53.4	55.4	58.6	61.2	64.8	70.3	75.9	88.4	104.3	126.1
65	45.0	46.6	49.2	51.5	52.2	52.5	53.05	54.4	56.4	59.6	62.3	65.8	71.4	77.1	89.8	106.0	128.1
66	45.8	47.5	50.1	52.4	53.1	53.5	53.99	55.3	57.4	60.6	63.3	66.9	72.6	78.3	91.2	107.6	130.1
67	46.7	48.4	51.0	53.4	54.1	54.4	54.92	56.3	58.4	61.6	64.4	68.0	73.8	79.6	92.7	109.3	132.1
68	47.5	49.2	51.9	54.3	55.0	55.3	55.86	57.2	59.3	62.6	65.4	69.1	74.9	80.8	94.1	111.0	134.1
69	48.4	50.1	52.8	55.2	55.9	56.2	56.79	58.2	60.3	63.7	66.4	70.2	76.1	82.1	95.5	112.6	136.1
70	49.2	51.0	53.7	56.1	56.8	57.2	57.73	59.1	61.3	64.7	67.5	71.3	77.3	83.3	96.9	114.3	138.1
71	50.1	51.8	54.6	57.0	57.8	58.1	58.67	60.1	62.3	65.7	68.5	72.4	78.4	84.6	98.4	115.9	140.1
72	50.9	52.7	55.5	58.0	58.7	59.0	59.61	61.0	63.2	66.7	69.6	73.5	79.6	85.8	99.8	117.6	142.1
73	51.8	53.6	56.4	58.9	59.6	60.0	60.55	62.0	64.2	67.7	70.6	74.6	80.8	87.0	101.2	119.3	144.1
74	52.7	54.5	57.3	59.8	60.6	60.9	61.49	62.9	65.2	68.7	71.7	75.6	81.9	88.3	102.7	120.9	146.1
75	53.5	55.3	58.2	60.7	61.5	61.8	62.43	63.9	66.2	69.7	72.7	76.7	83.1	89.5	104.1	122.6	148.0
76	54.4	56.2	59.1	61.7	62.4	62.8	63.37	64.9	67.2	70.8	73.8	77.8	84.2	90.8	105.5	124.3	150.0
77	55.2	57.1	60.0	62.6	63.4	63.7	64.32	65.8	68.1	71.8	74.8	78.9	85.4	92.0	106.9	125.9	152.0
78	56.1	58.0	60.9	63.5	64.3	64.7	65.26	66.8	69.1	72.8	75.9	80.0	86.6	93.3	108.4	127.6	154.0
79	56.9	58.8	61.8	64.4	65.2	65.6	66.20	67.7	70.1	73.8	76.9	81.1	87.7	94.5	109.8	129.3	156.0
80	57.8	59.7	62.7	65.4	66.2	66.5	67.15	68.7	71.1	74.8	78.0	82.2	88.9	95.7	111.2	130.9	158.0
81	58.7	60.6	63.6	66.3	67.1	67.5	68.09	69.6	72.1	75.8	79.0	83.3	90.1	97.0	112.6	132.6	160.0
82	59.5	61.5	64.5	67.2	68.0	68.4	69.04	70.6	73.0	76.9	80.1	84.4	91.2	98.2	114.1	134.3	162.0
83	60.4	62.4	65.4	68.2	69.0	69.4	69.99	71.6	74.0	77.9	81.1	85.5	92.4	99.5	115.5	135.9	164.0
84	61.3	63.2	66.3	69.1	69.9	70.3	70.93	72.5	75.0	78.9	82.2	86.6	93.6	100.7	116.9	137.6	166.0
85	62.1	64.1	67.2	70.0	70.9	71.2	71.88	73.5	76.0	79.9	83.2	87.7	94.7	102.0	118.3	139.3	168.0
86	63.0	65.0	68.1	70.9	71.8	72.2	72.83	74.5	77.0	80.9	84.3	88.8	95.9	103.2	119.8	140.9	170.0
87	63.9	65.9	69.0	71.9	72.7	73.1	73.78	75.4	78.0	82.0	85.3	89.9	97.1	104.5	121.2	142.6	172.0

88	64.7	66.8	69.9	72.8	73.7	74.1	74.73	76.4	78.9	83.0	86.4	91.0	98.2	105.7	122.6	144.3	174.0
89	65.6	67.7	70.8	73.7	74.6	75.0	75.68	77.3	79.9	84.0	87.4	92.1	99.4	106.9	124.0	145.9	176.0
90	66.5	68.6	71.8	74.7	75.6	76.0	76.63	78.3	80.9	85.0	88.5	93.1	100.6	108.2	125.5	147.6	178.0
91	67.4	69.4	72.7	75.6	76.5	76.9	77.58	79.3	81.9	86.0	89.5	94.2	101.7	109.4	126.9	149.3	180.0
92	68.2	70.3	73.6	76.6	77.4	77.8	78.53	80.2	82.9	87.1	90.6	95.3	102.9	110.7	128.3	150.9	182.0
93	69.1	71.2	74.5	77.5	78.4	78.8	79.48	81.2	83.9	88.1	91.6	96.4	104.1	111.9	129.7	152.6	184.0
94	70.0	72.1	75.4	78.4	79.3	79.7	80.43	82.2	84.9	89.1	92.7	97.5	105.3	113.2	131.2	154.3	186.0
95	70.9	73.0	76.3	79.4	80.3	80.7	81.39	83.1	85.8	90.1	93.7	98.6	106.4	114.4	132.6	155.9	188.0
96	71.7	73.9	77.2	80.3	81.2	81.6	82.34	84.1	86.8	91.1	94.8	99.7	107.6	115.7	134.0	157.6	190.0
97	72.6	74.8	78.2	81.2	82.2	82.6	83.29	85.1	87.8	92.2	95.8	100.8	108.8	116.9	135.5	159.3	192.0
98	73.5	75.7	79.1	82.2	83.1	83.5	84.25	86.0	88.8	93.2	96.9	101.9	109.9	118.2	136.9	160.9	194.0
99	74.4	76.6	80.0	83.1	84.1	84.5	85.20	87.0	89.8	94.2	97.9	103.0	111.1	119.4	138.3	162.6	196.0
100	75.2	77.5	80.9	84.1	85.0	85.4	86.16	88.0	90.8	95.2	99.0	104.1	112.3	120.6	139.7	164.3	198.0
101	76.1	78.4	81.8	85.0	86.0	86.4	87.12	88.9	91.8	96.3	100.0	105.2	113.4	121.9	141.2	165.9	200.0
102	77.0	79.3	82.7	85.9	86.9	87.3	88.07	89.9	92.8	97.3	101.1	106.3	114.6	123.1	142.6	167.6	202.0
103	77.9	80.2	83.7	86.9	87.8	88.3	89.03	90.9	93.8	98.3	102.2	107.4	115.8	124.4	144.0	169.2	204.0
104	78.8	81.1	84.6	87.8	88.8	89.2	89.99	91.9	94.8	99.3	103.2	108.5	116.9	125.6	145.4	170.9	206.0
105	79.6	82.0	85.5	88.8	89.7	90.2	90.94	92.8	95.7	100.4	104.3	109.6	118.1	126.9	146.9	172.6	208.0
106	80.5	82.8	86.4	89.7	90.7	91.1	91.90	93.8	96.7	101.4	105.3	110.7	119.3	128.1	148.3	174.2	210.0
107	81.4	83.7	87.4	90.7	91.6	92.1	92.86	94.8	97.7	102.4	106.4	111.8	120.4	129.4	149.7	175.9	212.0
108	82.3	84.6	88.3	91.6	92.6	93.1	93.82	95.7	98.7	103.4	107.4	112.9	121.6	130.6	151.1	177.6	214.0
109	83.2	85.5	89.2	92.5	93.5	94.0	94.78	96.7	99.7	104.5	108.5	114.0	122.8	131.9	152.6	179.2	216.0
110	84.1	86.4	90.1	93.5	94.5	95.0	95.74	97.7	100.7	105.5	109.5	115.1	124.0	133.1	154.0	180.9	218.0
111	85.0	87.3	91.0	94.4	95.5	95.9	96.70	98.7	101.7	106.5	110.6	116.2	125.1	134.3	155.4	182.6	220.0
112	85.8	88.3	92.0	95.4	96.4	96.9	97.66	99.6	102.7	107.5	111.7	117.3	126.3	135.6	156.9	184.2	222.0
113	86.7	89.2	92.9	96.3	97.4	97.8	98.62	100.6	103.7	108.6	112.7	118.4	127.5	136.8	158.3	185.9	224.0
114	87.6	90.1	93.8	97.3	98.3	98.8	99.58	101.6	104.7	109.6	113.8	119.5	128.6	138.1	159.7	187.6	226.0
115	88.5	91.0	94.7	98.2	99.3	99.7	100.54	102.5	105.7	110.6	114.8	120.6	129.8	139.3	161.1	189.2	228.0
116	89.4	91.9	95.7	99.2	100.2	100.7	101.50	103.5	106.7	111.7	115.9	121.7	131.0	140.6	162.6	190.9	230.0
117	90.3	92.8	96.6	100.1	101.2	101.7	102.46	104.5	107.7	112.7	116.9	122.8	132.1	141.8	164.0	192.6	232.0
118	91.2	93.7	97.5	101.1	102.1	102.6	103.43	105.5	108.7	113.7	118.0	123.9	133.3	143.1	165.4	194.2	234.0
119	92.1	94.6	98.5	102.0	103.1	103.6	104.39	106.4	109.7	114.7	119.1	125.0	134.5	144.3	166.8	195.9	236.0
120	93.0	95.5	99.4	103.0	104.0	104.5	105.35	107.4	110.7	115.8	120.1	126.1	135.7	145.6	168.3	197.6	238.0
121	93.9	96.4	100.3	103.9	105.0	105.5	106.31	108.4	111.6	116.8	121.2	127.2	136.8	146.8	169.7	199.2	240.0
122	94.7	97.3	101.2	104.9	105.9	106.4	107.28	109.4	112.6	117.8	122.2	128.3	138.0	148.1	171.1	200.9	242.0
123	95.6	98.2	102.2	105.8	106.9	107.4	108.24	110.3	113.6	118.9	123.3	129.4	139.2	149.3	172.6	202.6	244.0
124	96.5	99.1	103.1	106.8	107.9	108.4	109.21	111.3	114.6	119.9	124.4	130.5	140.3	150.6	174.0	204.2	246.0
125	97.4	100.0	104.0	107.7	108.8	109.3	110.17	112.3	115.6	120.9	125.4	131.6	141.5	151.8	175.4	205.9	248.0
126	98.3	100.9	105.0	108.7	109.8	110.3	111.14	113.3	116.6	121.9	126.5	132.7	142.7	153.0	176.8	207.6	250.0
127	99.2	101.8	105.9	109.6	110.7	111.2	112.10	114.3	117.6	123.0	127.5	133.8	143.9	154.3	178.3	209.2	252.0
128	100.1	102.8	106.8	110.6	111.7	112.2	113.07	115.2	118.6	124.0	128.6	134.9	145.0	155.5	179.7	210.9	254.0
129	101.0	103.7	107.8	111.5	112.6	113.2	114.03	116.2	119.6	125.0	129.6	136.0	146.2	156.8	181.1	212.6	256.0
130	101.9	104.6	108.7	112.5	113.6	114.1	115.00	117.2	120.6	126.1	130.7	137.1	147.4	158.0	182.5	214.2	258.0
131	102.8	105.5	109.6	113.4	114.6	115.1	115.96	118.2	121.6	127.1	131.8	138.2	148.5	159.3	184.0	215.9	260.0
132	103.7	106.4	110.6	114.4	115.5	116.0	116.93	119.1	122.6	128.1	132.8	139.3	149.7	160.5	185.4	217.6	262.0
133	104.6	107.3	111.5	115.3	116.5	117.0	117.90	120.1	123.6	129.2	133.9	140.4	150.9	161.8	186.8	219.2	264.0
134	105.5	108.2	112.4	116.3	117.4	118.0	118.87	121.1	124.6	130.2	134.9	141.5	152.0	163.0	188.3	220.9	266.0
135	106.4	109.1	113.3	117.2	118.4	118.9	119.83	122.1	125.6	131.2	136.0	142.6	153.2	164.3	189.7	222.6	268.0

136	107.3	110.0	114.3	118.2	119.4	119.9	120.80	123.1	126.6	132.2	137.1	143.7	154.4	165.5	191.1	224.2	270.0
137	108.2	111.0	115.2	119.1	120.3	120.9	121.77	124.0	127.6	133.3	138.1	144.8	155.6	166.8	192.5	225.9	272.0
138	109.1	111.9	116.2	120.1	121.3	121.8	122.74	125.0	128.6	134.3	139.2	145.9	156.7	168.0	194.0	227.6	274.0
139	110.0	112.8	117.1	121.0	122.2	122.8	123.71	126.0	129.6	135.3	140.2	147.0	157.9	169.3	195.4	229.2	276.0
140	110.9	113.7	118.0	122.0	123.2	123.7	124.67	127.0	130.6	136.4	141.3	148.1	159.1	170.5	196.8	230.9	278.0
141	111.8	114.6	118.9	123.0	124.2	124.7	125.64	128.0	131.6	137.4	142.4	149.2	160.2	171.8	198.3	232.6	280.0
142	112.7	115.5	120.0	123.9	125.1	125.7	126.66	129.0	132.6	138.5	143.5	150.3	161.4	173.0	199.7	234.2	282.0
143	113.5	116.3	120.8	124.9	126.1	126.7	127.59	129.9	133.6	139.5	144.5	151.4	162.6	174.2	201.1	235.9	284.0
144	114.4	117.2	121.8	125.9	127.1	127.6	128.52	130.9	134.6	140.5	145.5	152.5	163.8	175.5	202.5	237.6	286.0
145	115.3	118.2	122.7	126.8	128.0	128.6	129.54	132.0	135.7	141.6	146.6	153.6	164.9	176.7	204.0	239.2	288.0
146	116.3	119.2	123.7	127.8	129.0	129.5	130.46	132.9	136.6	142.6	147.6	154.7	166.1	178.0	205.4	240.9	290.0
147	117.2	120.1	124.6	128.7	129.9	130.5	131.44	133.9	137.6	143.6	148.8	155.8	167.3	179.2	206.8	242.6	292.0
148	118.1	121.0	125.5	129.6	130.9	131.4	132.38	134.8	138.6	144.7	149.8	156.9	168.5	180.5	208.2	244.2	294.0
149	119.0	121.9	126.4	130.6	131.8	132.5	133.40	135.8	139.6	145.7	150.8	158.0	169.6	181.7	209.7	245.9	296.0
150	119.9	122.8	127.4	131.6	132.8	133.4	134.39	136.8	140.7	146.7	151.9	159.1	170.8	183.0	211.1	247.6	298.0

BIBLIOGRAFÍA

1. Lydia Parziale, David T. Britt, Chuck Davis, "TCP/IP Tutorial and Technical Overview ", IBM RedBooks – Estados Unidos 2006.
2. Frankling D. Ohrtman Jr., "Softswitch - Architecture for VoIP", McGraw-Hill Companies, Estados Unidos 2004.
3. Kevin Wallace, "Cisco Voice over IP Fundamentals", Cisco Press, Estados Unidos 2008.
4. Juan Carlos Martín Castillo, "Instalaciones de telecomunicaciones", Editorial Editex, España 2009.
5. Cisco System, "CCDA 640-864 Official Cert Guide", Cisco Press, Estados Unidos 2011.
6. José Dordoigne, "Redes informáticas – Nociones fundamentales", Ediciones ENI, España 2011.
7. Douglas Coumer, "Computer networks and Internet", Prentice Hall, Estados Unidos 2009.
8. Cisco System, "Fundamentals of wireless LANs", Cisco Press, Estados Unidos 2007.
9. Cisco System, "CCNA security – implementing network security version1.0", Cisco Press, Estados Unidos 2009.