Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

ANÁLISIS DE LA FACTIBILIDAD TÉCNICA Y ECONÓMICA PARA LA MIGRACIÓN DE UNA RED METRO-ETHERNET EN STP A EAPS

Shelder Aurelio Monzón Bojorquez
Asesorado por el Ing. César Augusto Montejo Cardona

Guatemala, noviembre de 2017

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

ANÁLISIS DE LA FACTIBILIDAD TÉCNICA Y ECONÓMICA PARA LA MIGRACIÓN DE UNA RED METRO-ETHERNET EN STP A EAPS

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

SHELDER AURELIO MONZÓN BOJORQUEZ
ASESORADO POR EL ING. CESAR AUGUSTO MONTEJO CARDONA

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN ELECTRÓNICA

GUATEMALA, NOVIEMBRE DE 2017

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Pedro Antonio Aguilar Polanco
VOCAL I	Ing. Angel Roberto Sic García
VOCAL II	Ing. Pablo Christian de León Rodriguez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Jurgen Andoni Ramírez Ramírez
VOCAL V	Br. Oscar Humberto Galicia Nuñez
SECRETARIA	Inga. Lesbia Magalí Herrera López

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Sydney Alexander Samuels Milson
EXAMINADOR	Ing. Gustavo Adolfo Villeda Vásquez
EXAMINADOR	Ing. Guillermo Antonio Puente Romero
EXAMINADOR	Ing. Erwin Efraín Segura Castellanos
SECRETARIO	Ing. Pedro Antonio Aguilar Polanco

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

ANÁLISIS DE LA FACTIBILIDAD TÉCNICA Y ECONÓMICA PARA LA MIGRACIÓN DE UNA RED METRO-ETHERNET EN STP A EAPS

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 21 de marzo de 2011.

Shelder Aurelio Monzón Bojorquez

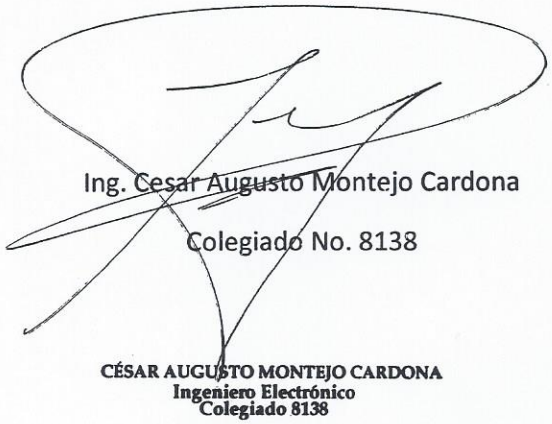
Guatemala, 04 de septiembre de 2017

Ingeniero Julio César Solares Peñate
Coordinador del Área de Electrónica
Escuela de Mecánica Eléctrica
Facultad de Ingeniería
USAC

Por este medio hago constar que he revisado el trabajo de tesis titulado: **ANÁLISIS DE LA FACTIBILIDAD TÉCNICA Y ECONÓMICA PARA LA MIGRACIÓN DE UNA RED METRO-ETHERNET EN STP A EAPS** del estudiante Shelder Aurelio Monzón Bojorquez que se identifica con número de carné 199811679.

El mismo cumple con los objetivos planteados y tanto yo como asesor así como el estudiante nos hacemos totalmente responsables por el contenido de este trabajo de tesis.

Atentamente,



Ing. Cesar Augusto Montejo Cardona

Colegiado No. 8138

CÉSAR AUGUSTO MONTEJO CARDONA
Ingeniero Electrónico
Colegiado 8138

FACULTAD DE INGENIERIA
Escuelas de Ingeniería Civil, Ingeniería Mecánica Industrial, Ingeniería Química, Ingeniería Mecánica Eléctrica, Técnica y Regional de Post-grado de Ingeniería Sanitaria.
Ciudad Universitaria, zona 12
Guatemala, Centroamérica

Guatemala, 18 de septiembre de 2017

Señor Director
Ing. Otto Fernando Andrino González
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Señor Director:

Por este medio me permito dar aprobación al Trabajo de Graduación titulado: **ANÁLISIS DE LA FACTIBILIDAD TÉCNICA Y ECONÓMICA PARA LA MIGRACIÓN DE UNA RED METRO-ETHERNET EN STP A EAPS**, desarrollado por el estudiante **Shelder Aurelio Monzón Bojorquez**, ya que considero que cumple con los requisitos establecidos.

Sin otro particular, aprovecho la oportunidad para saludarlo.

Atentamente,

ID Y ENSEÑAD A TODOS

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

Ing. Julio César Solares Peñate
Coordinador de Electrónica

NIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 50. 2017.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante; SHELDER AURELIO MONZÓN BOJORQUEZ titulado: ANÁLISIS DE LA FACTIBILIDAD TÉCNICA Y ECONÓMICA PARA LA MIGRACIÓN DE UNA RED METRO-ETHERNET EN STP A EAPS, procede a la autorización del mismo.

Ing. Otto Fernando Andrino González

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

GUATEMALA, 26 DE SEPTIEMBRE 2,017.

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

DTG. 534.2017

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al Trabajo de Graduación titulado: **ANÁLISIS DE LA FACTIBILIDAD TÉCNICA Y ECONÓMICA PARA LA MIGRACIÓN DE UNA RED METRO-ETHERNET EN STP A EAPS,** presentado por el estudiante universitario: **Shelder Aurelio Monzón Bojorquez,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

Ing. Pedro Antonio Aguilar Polanco
Decano

Guatemala, noviembre de 2017

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

/gdech

ACTO QUE DEDICO A:

Dios	Ya que por medio de su silenciosa pero transparente forma de expresarse guió mis pasos para alcanzar este éxito.
Mis padres	Francisca Medrano de Monzón y Luis Felipe Monzón de León, por sus enseñanzas y esfuerzo para que nuestra formación profesional fuera posible.
Mis hermanos	Wismar, Jhony y Danil, por todo el apoyo y consejos compartidos, una guía en mi caminar. Luis Gabriel porque es una invitación a que usted siga adelante.
Mis cuñadas	Fabiola, Susy y Glendy, por todo el aprecio que me han demostrado.
Mis sobrinos	Por su alegría y sonrisas que siempre me llenan.
Familiares	Que me brindaron apoyo y aliento para continuar.

Compañeros y amigos	Con quienes conviví los retos y las alegrías de la universidad, una agradable y única experiencia.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por abrirme las puertas a esta casa de educación y formación profesional.
Facultad de Ingeniería	Por la oportunidad que me brindaron de acceso al conocimiento.
Mis amigos de la facultad	Luis Carlos Morales, Julio Sosa, Victor Navas, Francisco Hernandez, Victor Morales, German Ventura, German Contreras, Hector Mejía, Nelson Santos, entre otros.
Ing. Cesar Montejo	Por su paciencia y su continuo apoyo en el desarrollo del presente trabajo de investigación.
Ing. Carlos de León	Por su confianza, amistad y apoyo durante los años de estudio en esta casa de estudio.
Ing. Pedro Mérida	Por su continua y frecuente motivación a continuar adelante.
Mis amigos de toda la vida	Por su motivación, alegría y apoyo a lo largo de nuestro caminar.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
$	Dólar
%	Porcentaje
Segs	Segundos

GLOSARIO

ACR (*Absolute category rating*) calificación de categoría absoluta.

ARP (*Adress resolution protocol*) protocolo de resolución de dirección.

Codec Es un programa, dispositivo o la combinación de ambos que hace posible transformar un flujo de señal y recuperarlo o descifrarlo posteriormente; es decir, codificar, decodificar de donde viene su nombre. Ampliamente usado en transmisión de señales de audio y video, también, usado para almacenar o cifrar información.

EAPS (*Ethernet automatic protection switching*) protección automática en conmutación Ethernet, fue inventado por Extreme Networks para mejorar la disponibilidad de los enlaces; es un esquema lineal de protección diseñado para proteger VLAN basado en redes Ethernet.

Ethernet Estándar que se basa en el estándar internacional IEEE 802.3, el cual define tres características importantes: cableado, señalización de nivel físico y los formatos de tramas de datos.

ETSI	(*European Telecommunications Standards Institute*) Instituto de Telecomunicaciones Estándares Europeo.
Extreme Networks	Empresa norteamericana fundada en 1996 dedicada al diseño, construcción e instalación de productos de red Ethernet *swtichs*, administradores de red y equipos de seguridad para microempresas hasta grandes operadores de telecomunicaciones.
Datagrama	Cada paquete o datagrama está compuesto por datos y encabezados, este último contiene la información para definir su enrutamiento, qué tipo de servicio se está usando, entre otros.
IP	(*Internet protocol*) protocolo de Internet.
ITU	(*International Telecommunication Union*) Unión Internacional de Telecomunicaciones.
Jitter	La fluctuación de fase de la trama o la variación del retraso, definido como la diferencia entre la trama con mayor retraso y la trama con retraso más bajo de una muestra de tramas considerada.
LAN	(*Local area network*) red de área local.
Loop	Bucle ocurre cuando todos los nodos de una red en topología anillo poseen información de un camino

	para alcanzar su destino por alguno de sus vecinos continúan entregándolo a sus vecinos creyendo que este podrá entregarlo al destinatario y conlleva a que la información nunca alcanza su destino y se queda en un ciclo repetitivo.
MAC	(*Media access control*) control de acceso al medio
MAN	(*Metropolitan area network*) red de área metropolitana
MEN	(*Metro ethernet network*) red metro Ethernet, se definirá como una arquitectura basada en el estándar Ethernet concentrada en un área metropolitana capaz de brindar servicios de conectividad, aplicación que incluyen telefonía IP y video IP.
MIT	(*Massachusetts Institute of Technology*) Instituto Tecnológico de Massachusetts
MOS	(*Mean opinion score*) puntuación de opinión promedio.
NAT	(*Network address translation*) traducción de direcciones de red
OSI	(*Open systems interconnection*) interconexión de sistemas abiertos.

Protocolo	Un protocolo de comunicaciones define en reglas o estándares la sintaxis, semántica y sincronización de la comunicación, también, los posibles métodos de recuperación de errores.
QoE	(*Quality of experience*) calidad de experiencia.
QoS	(*Quality of service*) calidad de servicio.
Router	O enrutadores, tienen la habilidad de mover los datos o paquetes desde el origen hacia el destino empleando su programación de configuración de red. A diferencia de los *switch,* estos pueden comunicar o enviar un paquete entre dos segmentos de red de forma autónoma.
RSTP	(*Rapid spanning tree protocol*) protocolo de árbol de expansión rápido que es una evolución a STP que reduce hasta en cinco veces el tiempo de respuesta a un cambio de topología.
STP	(*Spanning tree protocol*) protocolo de árbol de expansión opera sobre la capa de enlace que contribuye a evitar loops e identificar caminos alternos para alcanzar un destino.
Switch	Se encarga de trasladar las tramas desde un dispositivo de red a otro, y su principal función es asegurar o controlar el acceso al medio físico que

	brindan comunicación entre computadoras que pertenecen al mismo segmente de red. Cuando se requiere comunicar entre dos segmentos de red distintos es necesario el uso de un router o enrutador.
TCP	(*Transmission control protocol*) protocolo de control de transmisión.
TCP/IP	Modelo que describe un conjunto de guías para que un equipo pueda comunicarse en una red.
TIR	Tasa interna de retorno.
TTL	(*Time to live*) tiempo de vida.
UDP	(*User datagram protocol*) protocolo de datagrama de usuario.
VLAN	(*Virtual local area network*) red de área local virtual
VoIP	(*Voice over IP*) Cuando la voz es transportada en paquetes IP, es conocida como voz sobre Internet Protocol o VoIP por sus siglas en inglés (*voice over IP*), que no se refiere únicamente a un servicio sino a la tecnología que lo hace posible.
VPN	Valor presente neto.

WAN (*Wide area network*) red de área amplia.

RESUMEN

EAPS fue presentado originalmente como una solución de Extreme Networks para mejorar los tiempos de convergencia en redes de topología tipo anillo, pero debido a la cantidad de implementaciones de red metro-Ethernet y al creciente uso de servicios multimedia se ha hecho más popular su aplicación. Los operadores de telecomunicaciones, quienes ofrecen convencionalmente servicios de datos y servicios multimedia, han descubierto en EAPS una oportunidad para mejorar la tecnología de su red ya que los beneficios para los servicios prestados son atractivos. Telefonía, por ejemplo, es un servicio que los operadores suelen ofrecer, enviando la voz sobre protocolos de red como IP, por lo que suele referirse a este como voz sobre IP o VoIP, por sus siglas en inglés, *voice over IP*.

Una red en topología tipo anillo permite la comunicación por una ruta alterna ante la falla de uno de sus circuitos que evitan la afectación de los servicios del operador; en general, cualquier tipo de servicio se verá afectado si el tiempo para restablecer la conexión es muy elevado ya que tenderá a cortarse por falta de comunicación.

Los servicios de voz son aún más sensibles a fallas; por tratarse de un servicio en tiempo real, una conmutación prolongada causará una percepción de corte de llamada. Protocolos como *spanning tree protocol*, *rapid spanning tree protocol* o *Ethernet automatic protection switching* ofrecen técnicas que garantizan la convergencia a rutas alternas ante una falla. A lo largo de este trabajo se describirán estos protocolos, sus tiempos de convergencia y se

analizará si una migración de una red metro-Ethernet en STP a EAPS es factible técnica y económicamente.

OBJETIVOS

General

Analizar la factibilidad técnica y económica para la migración de una red metro-Ethernet con protocolo de protección STP a EAPS.

Específicos

1. Explicar los conceptos básicos de una red metro-Ethernet y los diferentes tipos de topologías.

2. Describir los modos de operación de los protocolos STP, RSTP y EAPS.

3. Realizar una comparación técnica de los protocolos STP, RSTP y EAPS.

4. Detallar los procedimientos necesarios para realizar la migración de una red metro-Ethernet en STP a EAPS.

5. Determinar la factibilidad técnica para la migración de una red metro-Ethernet en STP a EAPS.

6. Determinar la factibilidad económica para la migración de una red metro-Ethernet en STP a EAPS.

INTRODUCCIÓN

Los servicios de telefonía son con más frecuencia incluidos como parte del portafolio de servicios que los operadores de telecomunicaciones ofrecen a sus clientes, con la finalidad de volver más atractivo dicho portafolio. Sin embargo, algunos operadores aún poseen redes y tecnología que podrían no soportar completamente este tipo de servicios, ya que aunque la llamada se establezca, podría verse interrumpida ante algún evento o fallo en alguno de los circuitos de comunicación. Es ahí donde la imagen del operador podría verse impactada por este tipo de circunstancias y eventualmente tener repercusiones en la capacidad para atraer más clientes o retener a los existentes.

Los operadores de telecomunicaciones, por tanto, buscan que su infraestructura sea robusta, estable y con capacidad de recuperación ante una falla de forma automática para que servicios como la voz no sean afectados.

Para cumplir con estos requerimientos, los operadores frecuentemente optan por construir una red basada en estándares tanto para su infraestructura, topología y protocolos de comunicación, como lo es la implementación de red metro-Ethernet o MEN (del inglés *metro-Ethernet network*), que utiliza TCP/IP como protocolo base. Dichas redes además permiten la implementación de protocolos que se ocupan de la recuperación de la comunicación de forma automática y ágil que serán motivo de estudio en el presente trabajo.

A lo largo del trabajo se plantea una red Metro-Ethernet con topología tipo anillo que emplean *spanning tree protocol* para la protección de los servicios, para analizar si servicios como la telefonía pueden ser soportados con todos

sus requerimientos utilizando STP; además, se analiza la factibilidad de la migración a otros protocolos de protección para mejorar la protección como *rapid spanning tree protocol* y *ethernet automatic protection switching*.

1. INTRODUCCIÓN RED METRO-ETHERNET

En la actualidad, los requerimientos de los usuarios para comunicarse y emplear servicios multimedia como voz y video, adicionales a los servicios de transmisión de datos tradicionales, han hecho que muchos operadores de telecomunicaciones enfrenten el reto de construir una infraestructura capaz de soportar la demanda de usuarios, cumplir con los niveles de calidad que los clientes requieren, ser competitivos en el mercado y basarla en protocolos estándares que brinden servicios diversos de forma rápida, efectiva y dinámica.

Los operadores de telecomunicaciones buscan que su infraestructura sea robusta y estable, por lo que las topologías tipo anillo son una solución comúnmente implementada; el nombre de anillo se le da por la forma distribuida de los nodos que se caracterizan porque todos los elementos que lo componen son accesibles desde cualquier otro elemento por dos rutas que brindan el respaldo de la transmisión de los datos ante una falla en uno de los tramos de comunicación.

Los servicios multimedia requieren, además de respaldo y redundancia de los tramos de comunicación, que la conmutación o convergencia por la ruta alterna sea ágil y veloz ya que estos servicios son susceptibles a interrupciones o cortes; de no cumplir con esto es muy probable la pérdida de la comunicación en estos servicios.

Para cumplir con estos requerimientos combinados de redundancia, estabilidad y conmutación ágil los operadores frecuentemente optan por una

infraestructura en una red metro-Ethernet o MEN (del inglés *metro-Ethernet network*), que utiliza TCP/IP como protocolo base.

El protocolo TCP/IP es hoy en día considerado un protocolo estándar, flexible y con mucho potencial para múltiples aplicaciones, ampliamente utilizado para transporte de información en redes públicas, privadas y metropolitanas por su versatilidad de transferencia.

1.1. Modelo OSI y modelo TCP/IP

El modelo OSI es un marco de referencia para la definición de arquitecturas en la interconexión de los sistemas de comunicaciones y el modelo TCP/IP describe un conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que un equipo pueda comunicarse en una red. Ambos se basan en modelos de capas, un gran número de protocolos independientes basan sus conceptos en estos y la funcionalidad de las capas es muy similar, al punto de ser comparables entre ambos modelos.

1.1.1. Modelo OSI

Open systems interconnection (OSI) o interconexión de sistemas abiertos, fue creada por la Organización Internacional de Estándares como un marco y modelo de referencia para explicar cómo las diferentes tecnologías de red podrían trabajar juntos e interactuar. El modelo OSI no es un estándar que los protocolos de red deban seguir.

Cada capa tiene funciones específicas y trabajan juntas en el orden correcto para mover datos a lo largo de una red En la figura 1 se muestra el modelo OSI y las capas que lo componen.

Tabla I. **Capas del modelo OSI**

Modelo OSI
Capa aplicación
Capa de presentación
Capa de sesión
Capa de transporte
Capa de red
Capa de enlace de datos
Capa física

Fuente: elaboración propia.

- Capa física

La capa física en el modelo OSI se encarga de todos los aspectos para mover físicamente los datos de una computadora hacia la siguiente convirtiendo los datos de capas superiores en unos y ceros (1 y 0) para la transición sobre el medio. Además, define como se codifica la información en los medios de comunicación que se usan para la transmisión de los datos.

Dentro de esta capa se definen los estándares de cableado, conexiones inalámbricas y fibra óptica. Un ejemplo de equipo que trabaja en esta capa según el modelo OSI es el Hub.

- Capa enlace de datos

En esta capa se encapsulan los datos en tramas y es responsable de trasladar las tramas desde una computadora a otra; define lo necesario para mover las tramas de una computadora adyacente a otra, pero no puede mover las tramas a través de enrutadores. Un ejemplo de equipo que trabaja en esta capa según el modelo OSI es el *switch*; además, define lo relacionado al protocolo Ethernet y el protocolo punto a punto o PPP (del inglés *point-to-point protocol*), entre otros.

Para lograr este movimiento se requiere el apoyo de dos sub caps llamadas:

  - *Logical link control* (LLC) o control de enlace lógico: se encarga del direccionamiento de capa de enlace de datos, el control, la notificación de la dirección de flujo y de corrección de errores.

  - *Media access control* (MAC) o control de acceso al medio: determina qué equipo tiene acceso a los medios de comunicación de la red en un momento dado. Determina donde una trama termina y comienza la siguiente, esta función se denomina sincronización de trama.

- Capa de red

Es la responsable de mover los datos encapsulados y denominados como paquetes desde uno de los puntos finales de la red hasta el otro, a esto se le llama *end-to-end communications* o comunicación de extremo a extremo. Para

completar esta tarea de comunicación es necesaria una dirección lógica como una dirección IP.

Los dispositivos que actúan en esta capa son los *routers* o enrutadores. El enrutar o r*outing* es la habilidad de varios dispositivos de red y sus programas de configuración de mover los datos o paquetes desde el origen hacia el destino.

Toma los datos de capas superiores y los divide en segmentos que pueden ser enviados hacia las capas inferiores para la transmisión de los datos. Por consiguiente, al llegar a su destino los datos segmentados puedan ser armados de vuelta para las capas superiores. También, pone los segmentos en el orden correcto para que puedan ser armados para el destino.

Basado en la fiabilidad del transporte de los datos enviados se distinguen dos tipos de protocolos:

- Protocolos orientados a conexión como TCP, para asegurar que el destino reciba los segmentos. El receptor puede pedir la retransmisión de un paquete. Si el paquete no es notificado como recibido (ACK por sus siglas en inglés *acknowledge*), el transmisor envía de nuevo el paquete.

- Protocolos no orientados a conexión como UDP, para enviar los segmentos sin asegurar la entrega. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Existen aplicaciones para este tipo de protocolo como la

transmisión de audio y vídeo en tiempo real donde no se realizan retransmisiones por los requisitos de retardo que se tiene en estos casos.

- Capa de transporte

Este nivel entra en juego una vez que se ha producido el enlace entre nodos en la red. La comunicación es ya independiente de la red, siendo el nivel que enlaza lo que quiere transmitir el usuario con la información que hay que enviar. Este nivel tiene como misión ofrecer al usuario un enlace entre nodos fiable, entregando datos libres de error a la capa siguiente de sesión. Además, puede dividir la conexión para hacerla más rápida (varias conexiones al nivel de transporte). Los servicios ofrecidos incluyen el establecimiento del enlace de transporte, la transmisión de datos, así como la disolución del enlace.

- Capa de sesión

Es la responsable por el manejo del dialogo entre los dispositivos de red; establece, administra y termina las conexiones. En esta capa se define la comunicación que usarán los dispositivos, es decir, dúplex, simple o semi-dúplex; y proporciona procedimientos para el establecimiento de puestos de control, aplazamiento, la terminación y los procedimientos de reinicio o recuperación.

- Capa de presentación

Se preocupa por la forma en que la data es presentada a la red y maneja tres tareas principales:

- *Translation* o traducción: se encarga del cambio de los datos para que otro tipo de computador pueda entenderlo.

- *Compression* o compresión: hace que los datos sean lo más pequeños posible para enviar más datos en la misma cantidad de tiempo.

- *Encryption* o encripción: codifica los datos para protegerla de intercepciones o escuchas.

- Capa de aplicación

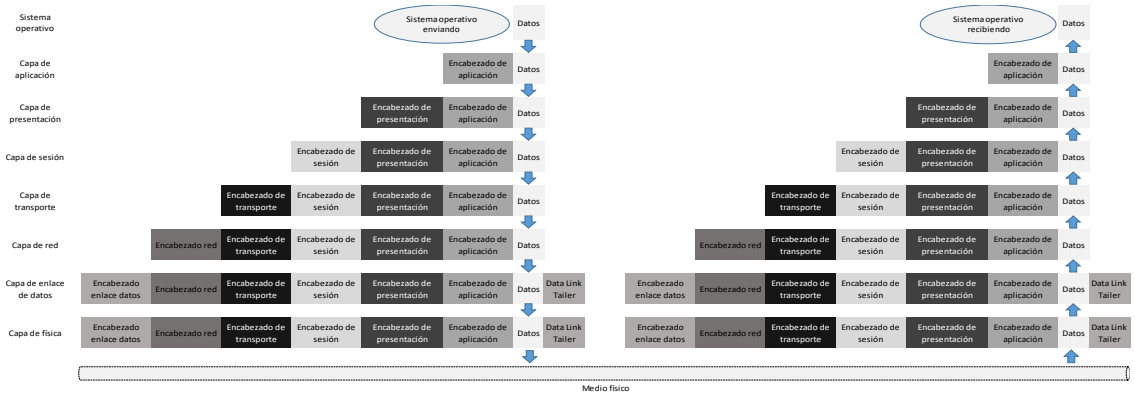
Contiene todos los servicios o protocolos necesarios para aplicaciones de programación o sistemas operativos puedan comunicarse hacia la red, por ejemplo:

Navegador web usa el protocolo HTTP (del inglés *hyper-text transport protocol*). Programas para manejo de correos usan POP3 (del inglés *post office protocol version 3*) para leer correos y SMTP (del inglés *simple mail transport protocol*) para enviar correos.

Cada capa del modelo OSI, excepto la capa física, agrega sus propios encabezados a la información o datos del sistema operativo origen en frente de los encabezados de capas previas. Estos encabezados contienen información que le describe a cada capa del modelo OSI que debe hacer con los datos. Además en la capa de enlace se agrega un encabezado secundario para proporcionar información que se ocupa de la corrección de errores, llamado *data link tailer*.

En la figura 1 se proporciona una ilustración de cómo se agrega cada encabezado de acuerdo a la capa del modelo OSI por la que van pasando los datos.

Figura 1. **Encabezados por cada capa del modelo OSI**



Fuente: elaboración propia.

1.1.2. Modelo TCP/IP

El modelo TCP/IP fue desarrollado en los años 70 y fue implantado en la primera red de área amplia, predecesora de la actual red Internet; desarrollada para el Departamento de Defensa de los Estados Unidos o DARPA (del inglés, *Defense Advanced Research Projects Agency*), y fue construido en torno al conjunto de protocolos TCP/IP, relacionados para que computadoras puedan comunicarse en una red.

El modelo TCP/IP, también se denomina a veces como modelo Internet, provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario. En la tabla II se muestra una ilustración del modelo TCP/IP.

Tabla II. **Capas del modelo TCP/IP**

Modelo TCP/IP
Capa de aplicación
Capa de transporte
Capa internet
Capa de interface de red

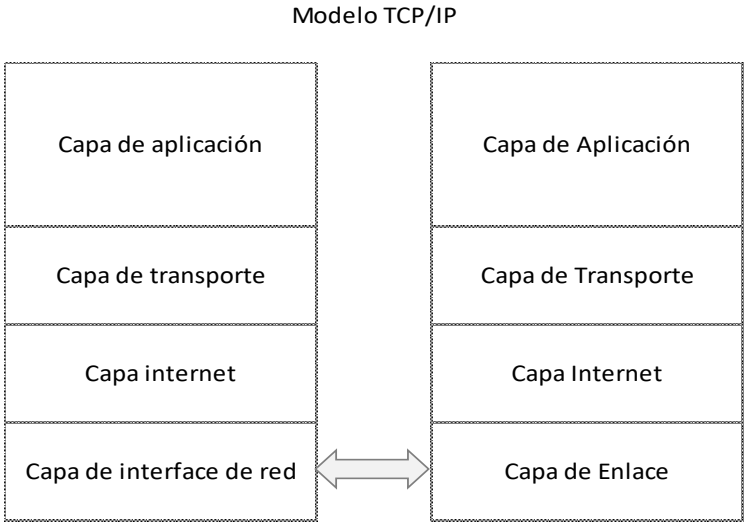
Fuente: elaboración propia.

- Capa de interface de red

Realiza gran parte del trabajo a lo que realiza MAC en la capa de enlace de datos y la capa física del modelo OSI. Una aclaración muy importante es que el protocolo TCP/IP no define lo que ocurre en la capa de interface de red. El conjunto de protocolos TCP/IP se basa en estándares creados por diversas organizaciones, estándares relativos a cómo codificar bits en los medios de comunicación para hacer el trabajo en esta capa; por lo que, algunos reconocen un nombre alterno para la última capa del modelo TCP/IP, como capa de enlace.

En la tabla III se muestra el nombre alterno que suele recibir la capa de interface de red o de enlace.

Tabla III. **Nombre alterno de las capas del modelo TCP/IP**



Fuente: elaboración propia.

- Capa de internet

Desempeña las mismas funciones que la capa de red del modelo OSI y muchas de las funciones de la subcapa de la capa de enlace de datos, LLC (*logical link control*). El protocolo principal de esta capa es *Internet protocol* (IP). Además, otro empleado es el *address resolution protocol* (ARP) con el que se desarrolla gran parte del trabajo de la subcapa LLC en lo que respecta al direccionamiento físico.

- Capa de transporte

La capa de transporte además cumple con las funciones de la capa de transporte y algunas de la capa de sesión del modelo OSI.

Protocolos como TCP y otros similares toman algunas de las funciones de la capa de sesión del modelo OSI como sincronizar los equipos de origen y de destino para establecer la sesión entre los respectivos equipos.

- Capa de aplicación

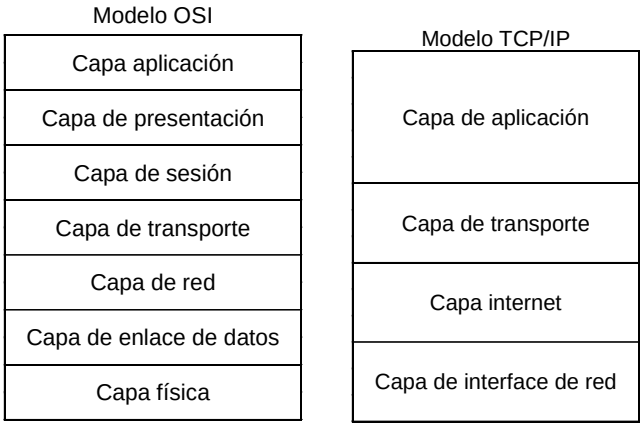
La capa de aplicación del modelo TCP/IP abarca las mismas funciones de las siguientes capas del modelo OSI:

  - Capa de aplicación
  - Capa de presentación
  - Capa de sesión

1.1.3. Comparación OSI y TCP/IP

Las principales similitudes entre los dos modelos es que ambos tienen una arquitectura basada en modelos de capas. Mientras el modelo OSI está compuesto por siete capas, el modelo TCP/IP tiene cuatro capas de abstracción. Aunque entre ambos modelos hay algunas capas con el mismo nombre, no necesariamente tienen la misma funcionalidad, como la capa de aplicación, que dependiendo del modelo incluye diferencias en los servicios. En la tabla IV se muestra una comparativa sobre lo que abarca cada capa del modelo TCP/IP con respecto a las capas del modelo OSI.

Tabla IV. **Comparativa modelo OSI y modelo TCP/IP**



Fuente: elaboración propia.

Mientras el modelo TCP/IP es considerado como el estándar sobre el cual la red de Internet fue desarrollada, el modelo OSI es un genérico estándar de protocolo independiente.

TCP/IP combina los asuntos de las capas presentación y sesión del modelo OSI dentro de su propia capa de aplicación; así mismo lo hace combinando el modelo OSI, las capas de enlace y física, dentro de su capa de Interface de red; por lo que TCP/IP se ve como un modelo más simple por la menor cantidad de capas.

El modelo OSI fue definido antes de implementar los protocolos, por lo que algunas funcionalidades necesarias de los protocolos no encuentran espacio, fallan o no existen dentro del modelo. En cambio, el modelo TCP/IP se creó después que los protocolos, por lo que se amolda a estas perfectamente.

1.2. Protocolo IP

El Protocolo Internet o IP (RFC 971, RFC 1122) por sus siglas en inglés (*Internet protocol*) es un protocolo de red no orientado a conexión donde su función principal es el envío de paquetes conmutados a través de redes físicas previamente enlazadas.

Los paquetes o datagramas son términos que típicamente en IP son usados de forma similar, por lo cual serán usados de forma indistinta a lo largo de este documento.

Su diseño fue pensado en la falta de garantía de la integridad y entrega de los paquetes al alcanzar el destino final; es decir, enfocado en manejarse por datagramas que serán manejados de forma independiente deberán contener toda la información para ser direccionado hasta su destino, y el protocolo, aunque lo ejecutará de la mejor forma buscando la mejor ruta por cada equipo que use IP.

Cuando los paquetes viajan con dirección a su destino, es posible que atraviese diferentes tipos de redes y debido a la separación por paquete es importante que se considere el máximo tamaño por cada paquete, a este se le conoce como MTU (*maximum transmission unit*). El protocolo IP no ofrece mecanismos para determinar si los paquetes alcanzaron o no su destino, es por eso que este protocolo brinda servicios a los protocolos de transporte como los protocolos TCP y UDP.

De acuerdo a la aplicación, el TCP es uno de los protocolos más empleados, por eso el término TCP/IP, combinando el protocolo de transporte TCP y el de red IP. Ya que en si solo el protocolo IP no presenta ningún tipo de

garantía sobre el envío, sobre su legitimidad, su orden, duplicidad o la falta del mismo al llegar al destino suele ser complementado por los protocolos de transporte como el TCP.

Cada paquete o datagrama está compuesto por datos (*data*) y encabezados (*header*); este último contiene la información para definir su enrutamiento, qué tipo de servicio se está usando, entre otros. En la tabla V se puede observar la estructura del datagrama y su longitud mínima de 20 octetos.

Tabla V. **Formato del datagrama IP**

<table>
<tr><td colspan="1">0</td><td colspan="1">1</td><td colspan="1">2</td><td colspan="1">3</td><td colspan="1">4</td><td colspan="1">5</td><td colspan="1">6</td><td colspan="1">7</td><td colspan="1">8</td><td colspan="1">9</td><td colspan="1">10</td><td colspan="1">11</td><td colspan="1">12</td><td colspan="1">13</td><td colspan="1">14</td><td colspan="1">15</td><td colspan="1">16</td><td colspan="1">17</td><td colspan="1">18</td><td colspan="1">19</td><td colspan="1">20</td><td colspan="1">21</td><td colspan="1">22</td><td colspan="1">23</td><td colspan="1">24</td><td colspan="1">25</td><td colspan="1">26</td><td colspan="1">27</td><td colspan="1">28</td><td colspan="1">29</td><td colspan="1">30</td><td colspan="1">31</td></tr>
<tr><td colspan="4">Versión</td><td colspan="4">Tamaño cabecera</td><td colspan="8">Tipo de servicio</td><td colspan="16">Longitud total</td></tr>
<tr><td colspan="16">Identificador</td><td colspan="3">Banderas</td><td colspan="13">Posición de Framento</td></tr>
<tr><td colspan="8">Tiempo de vida (time to live)</td><td colspan="8">Protocolo</td><td colspan="16">Suma de control de cabecera</td></tr>
<tr><td colspan="32">Dirección IP de origen</td></tr>
<tr><td colspan="32">Dirección IP de destino</td></tr>
<tr><td colspan="19">Opciones</td><td colspan="13">Relleno</td></tr>
<tr><td colspan="32">Datos ...</td></tr>
</table>

Fuente: elaboración propia.

- Versión

Se compone de 4 bits. Describe la versión de la cabecera Internet, en este se describe la versión 4, también conocido como IPv4.

- Tamaño de cabecera

Se compone de 4 bits. Describe la longitud de la cabecera en términos de palabras (*words*) equivalentes a 4 bytes o 32 bits, es decir, nótese que el valor

menor de este campo puede ser 5 si el datagrama está bien estructurado, correspondientes a los primeros 5 bloques de 32 bits (20 octetos) sin incluir los campos opciones y relleno.

- Tipo de servicio

Se compone de 8 bits. Proporciona una indicación de cómo debe ser manejado el paquete dentro de las redes, principalmente aporta la prioridad que se le debe proporcionar al paquete de acuerdo al servicio con respecto a paquetes de otros servicios.

- Longitud total

Se compone de 16 bits. Describe la longitud total del datagrama, medida en octetos en el cual se incluye tanto los datos como los encabezados. Ya que solo se compone de 16 bits, la mayor cantidad de octetos que puede contener un datagrama es de 2^16 = 65,536. Aunque es común que se envíen datagramas no mayores a 576 octetos a menos que se tenga seguridad que el destinatario pueda manejar datagramas mayores.

- Identificador

Se compone de 16 bits. Es un valor de identificación asignado por el remitente como ayuda en el ensamblaje de fragmentos de un datagrama.

- Banderas (*flags*) o indicadores

Se compone de 3 bits. Son empleados como indicadores de control y se refieren a la fragmentación realizada a la información, así:

- Bit 0. Reservado, debe ser 0
- Bit 1. Conocido como DF, no fragmentar (*don't fragment*)
  - 0 indica puede fragmentarse
  - 1 indica no fragmentar

- Bit 2. Conocido como MF más fragmentos (*more fragments*)
  Si es: 0 indica último fragmento
  1 indica más fragmentos

- Posición del fragmento

Se compone de 13 bits. Describe a que parte del datagrama pertenece este fragmento. La posición del fragmento se mide en unidades de 8 octetos (64 bits). El primer fragmento tiene posición 0.

- Tiempo de vida (*time to live*)

Se compone de 8 bits. Este campo sirve para identificar el tiempo máximo que permanecerá en la red un datagrama dentro de la red de Internet. Es medido en segundos. Si este valor es cero, el datagrama debe ser destruido. La intensión de esto es asegurar que los datagramas que sean imposibles de entregar sean descartados y limitar el máximo período que existirá el datagrama dentro de la red. El tiempo máximo que un datagrama puede existir es 255 segundos.

- Protocolo

Se compone de 8 bits. Se refiere a los protocolos que debe entregar la información en las capas superiores, para esta identificación se utiliza la

numeración asignada en el RFC 790. Por ejemplo: ICMP (1), TCP (6), UDP (17).

- Suma de control de cabecera

Se compone de 16 bits. Dado que algunos campos de la cabecera cambian (p. ej. el tiempo de vida), esta suma es recalculada y verificada en cada punto donde la cabecera internet es procesada. Aunque es fácil de emplear y adecuada es provisional y puede ser reemplazada.

- Dirección de origen

Se compone de 32 bits. Describe la dirección IP origen y se compone por un identificador de red (*netid*) y por un identificador de host (*hostid*). Para esta dirección IP existe una clasificación tipo A, B, C y D.

- Dirección de destino

Se compone de 32 bits. Describe la dirección IP destino y se compone por un identificador de red (*netid*) y por un identificador de host (*hostid*). Para esta dirección IP existe una clasificación tipo A, B, C y D.

- Opciones

El campo puede que aparezca o no en un datagrama IP y la existencia de este campo viene determinada por la longitud de la cabecera. Si el encabezado es mayor de cinco, por lo menos existe una opción. Aunque un host no está obligado a poner opciones, puede aceptar y procesar opciones recibidas en un

datagrama. El campo 'Opciones' es de longitud variable. Pueden existir cero o más opciones. Existen dos casos para el formato de una opción:

- Caso 1: un solo octeto de tipo-opción.
- Caso 2: un octeto tipo-opción, un octeto longitud-opción y los octetos correspondientes a los datos de opción.

El octeto longitud-opción es la cuenta del octeto tipo-opción y el octeto longitud-opción, así como los octetos de datos de opción.

El octeto tipo-opción tiene 3 campos, 1 bit indicador de copiado, 2 bits para definir la clase de opción y 5 bits para definir el número de opción.

- Relleno

El valor de relleno se usa para asegurar que la cabecera internet ocupa un múltiplo de 32 bits. El valor de relleno es cero.

- Datos

Este se refiere a la información que fue fragmentada y separada que será enviada dentro de los datagramas; como se ha descrito, debe tener una longitud a depender de los medios físicos.

- Direcciones IP

Las direcciones IP son identificadores numéricos lógicos y jerárquicos a las interfaces de las máquinas origen y destino usadas por los equipos

intermedios para determinar el tramo de la red por el cual será enviado el paquete o datagrama cuando es empleado el protocolo de Internet (IP). No se debe confundir este direccionamiento IP con la dirección MAC que se refiere a un número físico asignado por fabricantes de forma única a las tarjetas o dispositivos de red, mientras que las direcciones se pueden cambiar.

Las direcciones IP se expresan por un número binario de 32 bits, en el caso de IP versión 4 o IPv4, está compuesta por una dirección de red, seguida de una dirección de subred y de una dirección de host. Para su comprensión estos 32 bits se dividen en 4 octetos, y cada octeto se convierte a decimal, con lo que cada octeto puede variar entre 0 a 255 (el número binario de 8 bits más alto es 11111111 = 255 en decimal); el punto '.' es empleado para separar cada octeto. Ejemplo de direccionamiento IPv4: 192.168.10.255 o 192.168.010.255; en la notación decimal, los ceros iniciales de cada octeto pueden ser omitidos.

- Direcciones públicas

Cuando un usuario se conecta desde su hogar a Internet, requiere emplear una IP pública para enviar sus solicitudes de conexión hacia Internet, regularmente, el usuario no tiene dicha IP configurada directamente, ya que estás son únicas y son asignadas a proveedores de Internet. Para asegurar que las IP sean únicas existen entidades encargadas de ciertas regiones del mundo para la asignación de dicho direccionamiento público; para la región de Latinoamérica y El Caribe la entidad se llama LACNIC por sus siglas en inglés, *Latin America & Caribbean Network Information Center* (Registros de Direcciones de Internet para Latinoamérica y el Caribe).

- Direcciones privadas

Existen ciertos rangos de direccionamiento IP que no pueden ser asignadas como IP públicas; este segmento de direcciones IP es conocido como direcciones privadas; estas direcciones pueden ser utilizadas por los hosts que usan traducción de dirección de red (*network address translation* – NAT) para conectarse a una red pública como Internet. En una misma red no pueden existir dos direcciones iguales, pero sí se pueden repetir en dos redes privadas sin conexión entre sí o que se conecten mediante el protocolo NAT. Existen tres clases de direcciones de acuerdo a la cantidad de hosts disponibles; aunque históricamente se reconocían 5 clases en el desarrollo de este documento se trabajarán con base en las 3 principales clases. En la tabla VI se muestran las 3 clases principales, A, B y C, el uso de los octetos, cantidad de redes, host por red y su máscara de red.

Tabla VI. **Clases de direcciones IP**

Clase	1er octeto					2do octeto	3er octeto	4to octeto	Rango	No. de Redes	No. de host por red	Máscara de red
	1	2	3	4	5-8	9-16	17-24	25-32				
A	1	Identificador de red (7 bits)				Identificador de Nodo (24 bits)			1.0.0.0 - 127.255.255.255	126	16,777,214	255.0.0.0
B	1	0	Identificador de red (14 bits)				Identificador de Nodo (16 bits)		128.0.0.0 - 191.255.255.255	16,384	65,534	255.255.0.0
C	1	1	0	Identificador de red (21 bits)				Identificador de Nodo (8 bits)	192.0.0.0 - 223.255.255.255	2,097,152	254	255.255.255.0

Fuente: elaboración propia.

La clase A contiene 7 bits para direcciones de red, con lo que permite tener hasta 126 redes, con 16.777.214 ordenadores cada una. Las direcciones estarán comprendidas entre 0.0.0.0 y 127.255.255.255, y la máscara de subred será 255.0.0.0.

La clase B contiene 14 bits para direcciones de red y 16 bits para direcciones de hosts. El número máximo de redes es 16 384 redes, con 65 534 ordenadores por red. Las direcciones estarán comprendidas entre 128.0.0.0 y 191.255.255.255, y la máscara de subred será 255.255.0.0.

La clase C contiene 21 bits para direcciones de red y 8 para hosts, lo que permite tener un total de 2 097 152 redes, cada una con 254 ordenadores. Las direcciones estarán comprendidas entre 192.0.0.0 y 223.255.255.255 y la máscara de subred será 255.255.255.0.

1.3. Qué es una red metro-Ethernet

Para definir una red metro-Ethernet se iniciará por términos básicos para avanzar en la comprensión hasta alcanzar una definición.

- Red de área local (LAN)

Una red de área local (LAN) es un grupo de ordenadores o computadoras en un área localizada con el fin de compartir recursos y comunicarse entre sí bajo un estándar definido; dicha comunicación emplea diferentes tecnologías, aunque la más utilizada es la Ethernet.

- Red de área local virtual (VLAN)

Una red de área local virtual o VLAN por sus siglas en inglés *(virtual local area network*) es un método utilizado para crear a nivel lógico, LAN separadas e independientes, aunque transiten en la misma red a nivel física; es decir, varias VLAN pueden coexistir en un único *switch* físico, pero no tiene comunicación entre estas a no ser que un *router* les provea comunicación. Son utilizadas con

frecuencia por administradores ya que reducen el dominio de difusión y separa segmentos lógicos de una red de área local, por ejemplo, por departamentos de una empresa o clientes.

- Ethernet

Ethernet es un estándar que se basa en el estándar internacional IEEE 802.3, el cual define tres características importantes: cableado, señalización de nivel físico y los formatos de tramas de datos.

Ethernet por definición, es un estándar de acceso múltiple por detección de portadora con detección de colisiones o CSMA/CD por sus siglas en inglés (*carrier sense multiple access with collision detection*); para entender lo que esto significa habrá que remontarse a 1970 cuando Robert Metcalfe era un estudiante recién graduado en el Instituto Tecnológico de Massachusetts o MIT, por sus siglas en inglés (*Massachusetts Institute of Technology*).

Robert presentó en su tesis doctoral una idea simple, en la cual las estaciones antes de transmitir deberían detectar si el canal de comunicación está en uso; es decir, la onda portadora, y si estaba ocupada esperaría a que la estación activa completará su comunicación; además definía que se estaría vigilando continuamente el medio físico por si se producía alguna colisión, en cuyo caso se retransmitiría más tarde. En 1973 trabajando para Xerox en Palo Alto, Metcalfe, completó sus investigaciones y desarrollo el protocolo Ethernet con todas las características esenciales de la actualidad; aunque en esa época tenía una topología de bus y funcionaba a 2,94 Mb/s sobre conductores tipo coaxial. En la tabla VII se muestra un resumen sobre la evolución del estándar Ethernet.

Tabla VII. **Evolución de versiones 802.3**

Estándar Ethernet	Fecha	Descripción
Ethernet experimental	1972 (patentado en 1978)	2,85 Mbit/s sobre cable coaxial en topología de bus.
Ethernet II (DIX v2.0)	1982	10 Mbit/s sobre coaxial fino (thinnet) - La trama tiene un campo de tipo de paquete. El protocolo IP usa este formato de trama sobre cualquier medio.
IEEE 802.3	1983	10BASE5 10 Mbit/s sobre coaxial grueso (thicknet). Longitud máxima del segmento 500 metros - Igual que DIX salvo que el campo de Tipo se substituye por la longitud.
802.3a	1985	10BASE2 10 Mbit/s sobre coaxial fino (thinnet o cheapernet). Longitud máxima del segmento 185 metros
802.3b	1985	10BROAD36
802.3c	1985	Especificación de repetidores de 10 Mbit/s
802.3d	1987	FOIRL (Fiber-Optic Inter-Repeater Link) enlace de fibra óptica entre repetidores.
802.3e	1987	1BASE5 o StarLAN
802.3i	1990	10BASE-T 10 Mbit/s sobre par trenzado no blindado (UTP). Longitud máxima del segmento 150 metros.
802.3j	1993	10BASE-F 10 Mbit/s sobre fibra óptica. Longitud máxima del segmento 1000 metros.
802.3u	1995	100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet a 100 Mbit/s con auto-negociación de velocidad.
802.3x	1997	Full Duplex (Transmisión y recepción simultáneos) y control de flujo.
802.3y	1998	100BASE-T2 100 Mbit/s sobre par trenzado no blindado(UTP). Longitud máxima del segmento 100 metros
802.3z	1998	1000BASE-X Ethernet de 1 Gbit/s sobre fibra óptica.
802.3ab	1999	1000BASE-T Ethernet de 1 Gbit/s sobre par trenzado no blindado
802.3ac	1998	Extensión de la trama máxima a 1522 bytes (para permitir las "Q-tag") Las Q-tag incluyen información para 802.1Q VLAN y manejan prioridades según el estandar 802.1p.
802.3ad	2000	Agregación de enlaces paralelos.
802.3ae	2003	Ethernet a 10 Gbit/s ; 10GBASE-SR, 10GBASE-LR
IEEE 802.3af	2003	Alimentación sobre Ethernet (PoE).
802.3ah	2004	Ethernet en la última milla.
802.3ak	2004	10GBASE-CX4 Ethernet a 10 Gbit/s sobre cable bi-axial.
802.3an	2006	10GBASE-T Ethernet a 10 Gbit/s sobre par trenzado no blindado (UTP)
802.3ap	en proceso (draft)	Ethernet de 1 y 10 Gbit/s sobre circuito impreso.
802.3aq	en proceso (draft)	10GBASE-LRM Ethernet a 10 Gbit/s sobre fibra óptica multimodo.
802.3ar	en proceso (draft)	Gestión de Congestión
802.3as	en proceso (draft)	Extensión de la trama

Fuente: elaboración propia.

Dentro de las características de cableado y señalización se encuentran las definiciones físicas del tipo de trenzado de los cables, transporte de los datos hacia y fuera del dispositivo, codificado y descodificado de los datos, detección de portadora, detección de colisiones, conectores, medios físicos a emplear (eléctricos, ópticos), entre otros.

El estándar Ethernet además define lo que se refiere al formato de la trama Ethernet, es a lo que se denomina *frame*. En la tabla VIII se muestra la estructura de la trama de 802.3 Ethernet.

Tabla VIII. **Estructura de la trama de 802.3 Ethernet**

<table>
<tr><td>Preámbulo</td><td>Delimitador de inicio de trama</td><td>MAC de destino</td><td>MAC de origen</td><td>802.1Q etiqueta (opcional)</td><td>Ethertype (Ethernet II) o longitud (IEEE 802.3)</td><td>Payload</td><td>Secuencia de comprobación (32-bit CRC)</td><td>Gap entre frames</td></tr>
<tr><td>7 Bytes</td><td>1 Byte</td><td>6 Bytes</td><td>6 Bytes</td><td>(4 Bytes)</td><td>2 Bytes</td><td>De 46 (o 42) hasta 1500 Bytes</td><td>4 Bytes</td><td>12 Bytes</td></tr>
<tr><td colspan="2"></td><td colspan="6">64 - 1522 Bytes</td><td></td></tr>
<tr><td colspan="8">72 - 1530 Bytes</td><td></td></tr>
<tr><td colspan="9">84 - 1542 Bytes</td></tr>
</table>

Fuente: elaboración propia.

- Preámbulo (7 bytes)

Indica el inicio de la trama y se emplea para que el dispositivo que lo recibe detecte una nueva trama y se sincronice.

- Delimitador de inicio de trama (1 byte)

Marca el inicio del *frame* a partir de este.

- MAC de destino y origen (6 bytes cada uno)

Representan las direcciones físicas de los dispositivos a donde van dirigidos los datos y origen de los datos.

- La etiqueta (campo opcional – 4 bytes)

Empleado para indicar que el *frame* pertenece a una VLAN o bien la prioridad en IEEE P802.1p.

- *Ethernetype* (2 bytes)

Indica con que protocolo están encapsulados los datos que contiene la *Payload*, en caso de que se usase un protocolo de capa superior.

- *Payload* (46 o 42 hasta 1 500 bytes)

Es el espacio para el contenido de los datos o bien para las cabeceras de otros protocolos de capas superiores que pudieran formatear a los datos que se tramiten (IP, TCP, etc.). Tiene un mínimo de 46 bytes (o 42 si es la versión 802.1Q) hasta un máximo de 1 500 bytes.

- Secuencia de comprobación (4 bytes)

Contiene un valor de verificación CRC (control de redundancia cíclica). El emisor calcula el CRC de toda la trama, desde el campo destino al campo CRC suponiendo que vale 0. El receptor lo recalcula, si el valor calculado es 0, la trama es válida.

- *Gap* (12 bytes)

Son 12 bytes vacíos con el objetivo de espaciado entre tramas.

A partir del 2003 oficialmente se estandarizaron los detalles para alcanzar los 10 Gbit/s lo cual dio más popularidad a la tecnología Ethernet, ampliando la aceptación para ubicarse a niveles de redes de área amplia o WAN por sus siglas en inglés (*wide area network*).

- Red de área amplia (WAN)

Una red de área amplia (WAN), por sus siglas en inglés (*wide area network*), se define como la interconexión y comunicación de varios ordenadores en diferentes ubicaciones físicas, desde distintos niveles en un edificio hasta incluso varios continentes; en cada ubicación se puede identificar una red de área local (LAN).

- Red de área metropolitana (MAN)

El término red de área metropolitana o MAN, por sus siglas en inglés (*metropolitan area network*), se define como una red que une o comunica diferentes LAN, pero que están dispersas en un área metropolitana (como una ciudad, concentrada en un par de decenas de kilómetros) utilizando diferentes medios de comunicación como cobre, fibra o microondas y diferentes tecnologías como ATM, *frame relay*; entre estos también Ethernet.

- Red metro-Ethernet

En resumen, Ethernet es un estándar definido en principio para redes de área local (LAN) y redes de área amplia (WAN), dedicado a la definición de características de cableado, señalización de nivel físico y los formatos de tramas de datos.

Una red metro-Ethernet se definirá como una arquitectura basada en el estándar Ethernet concentrada en un área metropolitana capaz de brindar servicios de conectividad, aplicación, que incluye telefonía IP y video IP; estos últimos en particular resultan ser sensibles a algunas características de redes

Ethernet como el retardo y *jitter*, fenómenos que serán explicados más adelante.

Además, es común al referirse a una red metro-Ethernet como MEN por sus siglas en inglés (*metro-Ethernet network*), también como red de área metropolitana o MAN por sus siglas en inglés (*metropolitan area network*).

1.4. Servicios en redes metro-Ethernet

Dentro de una red metro-Ethernet, como se ha mencionado pueden ser transferidos diferentes tipos de servicios, que pueden clasificarse basados en lo requerimientos para que su calidad no se vea afectada por las condiciones de la red de transporte.

- Servicios en tiempo real, *real time* en inglés

La definición de los servicios de tiempo real se refiere a que la información debe ser transmitida en el momento cuando se genera; no hay oportunidad a retransmisiones ya que esto podría producir retrasos en la transmisión, por lo que debe ser entregada con la misma velocidad con la que se produce. Dentro de estos se encuentran los servicios de voz o video. La entrega de servicios *real time* sobre redes IP representan una alternativa de crecimiento para los proveedores de servicios.

La convergencia de las comunicaciones de empresa – voz, datos y video – sobre redes IP es una fuerte tendencia. Esto es debido a que las soluciones que más mercados ofrecen integrando voz, datos y también video, aportan importantes beneficios para las empresas y sus usuarios, como ahorros en

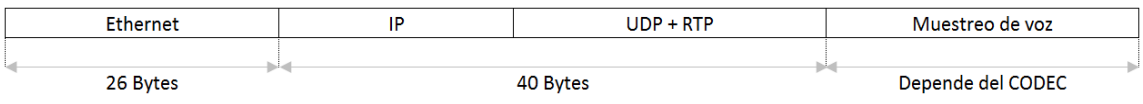
llamadas, simplificación infraestructura de comunicaciones, optimización de la gestión, entre otros.

Cuando la voz es transportada en paquetes IP, es conocida como voz sobre *Internet protocol* o VoIP por sus siglas en inglés (*voice over IP*). Algunos definen que VoIP no se refiere únicamente a un servicio sino más bien a la tecnología que permite encapsular en IP la voz, sin emplear los conmutadores convencionales de la red telefónica pública conmutada o PSTN por sus siglas en inglés (*public switched telephone network*).

Ya que la voz en su forma natural es analógica es necesario someterla a un proceso de digitalización, con el fin de codificarla en forma digital y transmitir el contenido digital por las redes IP, segmentando la información en datagramas o paquetes. El proceso de digitalización permite reducir el tamaño de los paquetes y agiliza su envío, por medio de técnicas de muestreo y codificación de la voz.

Las muestras de voz digitalizadas son encapsuladas en un protocolo de transporte en tiempo real o RTP (*real-time transport protocol*) luego en UDP (*user datagrama protocol*) antes de ser enviadas en una trama IP. En la figura 2 se muestra como se conforma una trama VoIP.

Figura 2. **Trama VoIP**



Fuente: elaboración propia.

Como se ve en la trama VoIP el tamaño en bytes de la muestra de la voz dependerá del códec (codificador-decodificador) para transmitir la voz a través de la red de datos, encargándose de garantizar la codificación y compresión del audio para su posterior decodificación y descompresión antes de generar un sonido utilizable.

Según el códec utilizado en la transmisión, se utilizará más o menos ancho de banda. La cantidad de ancho de banda utilizada suele ser directamente proporcional a la calidad de los datos transmitidos.

Los códec más utilizados en VoIP son G.711, G.723.1 y G.729, que son especificados por la ITU, *telecommunication standardization sector* o ITU-T por sus siglas en inglés, que es uno de los tres sectores o divisiones de la Unión Internacional de Telecomunicaciones o ITU (International Telecommunication Union). En la tabla II se muestra el flujo de datos que proporcionan para la transmisión de cada uno de estos códec.

Tabla IX. **Ancho de banda por codec para VoIP**

Codec	Algoritmo utilizado	Flujo de datos
G.711	PCM (pulse code modulation)	64 Kbps
G.726	ADPCM (adaptive differential pulse code modulation)	16, 24, 32, 40 Kbps
G.728	LD-CELP (low delay code excited linear prediction)	16 Kbps
G.729	CS-ACELP (conjugate structure algebraic CELP)	8 Kbps
G.723.1	MP-MLQ (multi-pulse maximum likelihood Qquantization)	6,3 Kbps 5,3 Kbps
	ACELP (algebraic code excited linear prediction)	6,3 Kbps 5,3 Kbps

Fuente: elaboración propia.

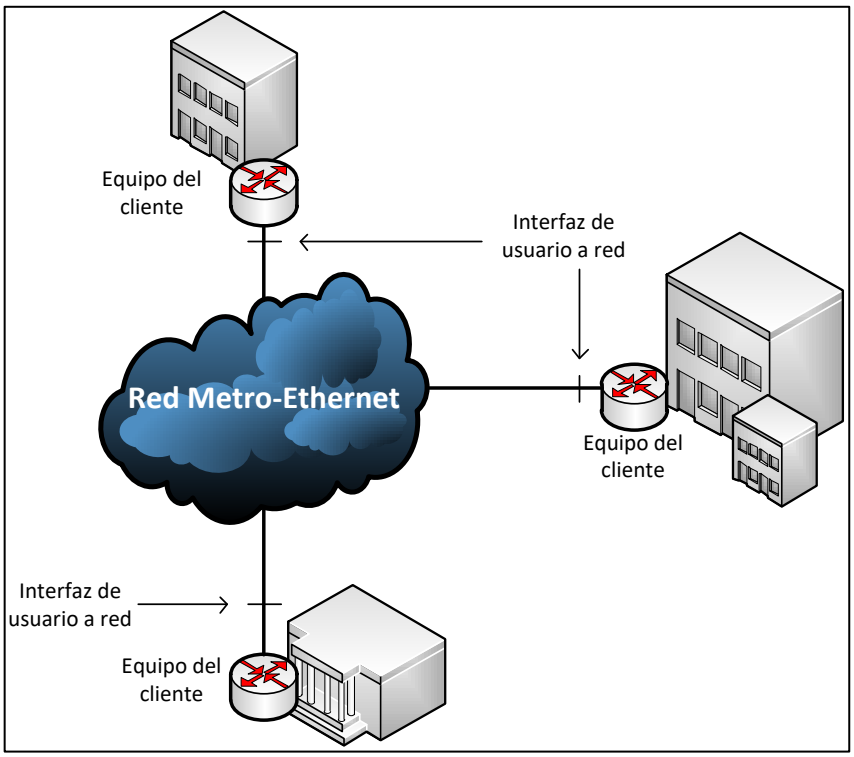
- Servicios no en tiempo real, o *non real time* en inglés

El concepto de *non real time* se refiere a que la entrega de la información no tiene razón de suceder con la misma velocidad con la que se genera. Dentro de estos se encuentran la transmisión tradicional de datos, o envío de información sobre protocolos de capas superiores como navegación hacia internet HTTP, o envió de correos SMTP. Comúnmente servicios como estos son soportados en la capa de transporte por protocolos como TCP que, como se ha mencionado, garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron, ya que el tiempo de transmisión para estos servicios no es un factor de interés al hablar de su calidad.

1.5. Características de una red metro-Ethernet

Todos los servicios Ethernet comparten algunos atributos, pero existen algunas diferencias dependiendo del tipo de servicio. Un modelo básico para un servicio Ethernet se muestra en la figura 3 sobre una red metro-Ethernet.

Figura 3. **Modelo básico para un servicio Ethernet**



Fuente: elaboración propia, empleando Visio.

Un servicio Ethernet es provisto por un proveedor de red metro-Ethernet o RME. En el modelo básico se ve que un Equipo del cliente o EC, se conecta a esta red por medio de la una interfaz de usuario a red o IUR, empleando como estándares de interfaces Ethernet de 100 Mbps o 1 Gbps, entre otras.

La definición de los atributos son los que definen las capacidades de cada tipo de servicio, que pueden ser agrupados o clasificados. A continuación, se señalan los diferentes atributos agrupados que pueden definir los servicios Ethernet.

- Interface física Ethernet

En la IUR, la interfaz física Ethernet tiene algunos atributos de servicio asociados:

- Medio físico

El atributo de medio físico de la IUR específica la interface física de acuerdo a los estándares de la IEEE 802.3, por ejemplo, 10 BaseT, 100 BaseT y 1000 BaseSX.

- Velocidad

El atributo de velocidad de la IUR especifica la velocidad estándar Ethernet: 10 Mbps, 100 Mbps, 1 Gbps y 10 Gbps.

- Modo

El atributo de modo de la IUR específica que tipo de negociación de velocidad es soportada por dicha interfaz: *full* o *half duplex* o inclusive de negociación automática.

- Capa medio control de acceso (MAC, por sus siglas en inglés)

El atributo de MAC de la IUR especifica o indica el tipo de capa MAC soportado; actualmente, las capas MAC soportadas que son especificadas en los estándares IEEE 802.3.

- Perfil de ancho de banda

También, se define como atributo para definir los servicios Ethernet el perfil de ancho de banda que puede ser aplicado a la IUR. Un perfil de ancho de banda es un límite sobre la tasa de transferencia sobre la IUR. Estos perfiles son posibles por las tramas que ingresan y egresan hacia y fuera de la red; un ejemplo de un perfil de ancho de banda es la tasa de información comprometida, CIR por sus siglas en inglés (*committed information rate*) para un circuito virtual permanente o PVC por sus siglas en inglés (*permanent virtual circuit*) en una red *frame relay*.

Los perfiles de ancho de banda para un servicio Ethernet consiste de los siguientes cuatro parámetros de tráfico.

- Tasa de Información comprometida, CIR por sus siglas en inglés (*committed information rate*): es la cantidad promedio de información que se ha transmitido, teniendo en cuenta los retardos, pérdidas, etc.

- Tamaño de ráfaga comprometido, CBS por sus siglas en inglés (*committed burst size*): es el tamaño de la información utilizado para obtener el CIR respectivo.

- Tasa de información de exceso, EIR por sus siglas en inglés (*excess information rate*): especifica la cantidad de información mayor o igual que el CIR, hasta el cual las tramas son transmitidas sin pérdidas.

- Tamaño de ráfaga de exceso, EBS por sus siglas en inglés (*excess burst size*): es el tamaño de información que se necesita para obtener el EIR determinado.

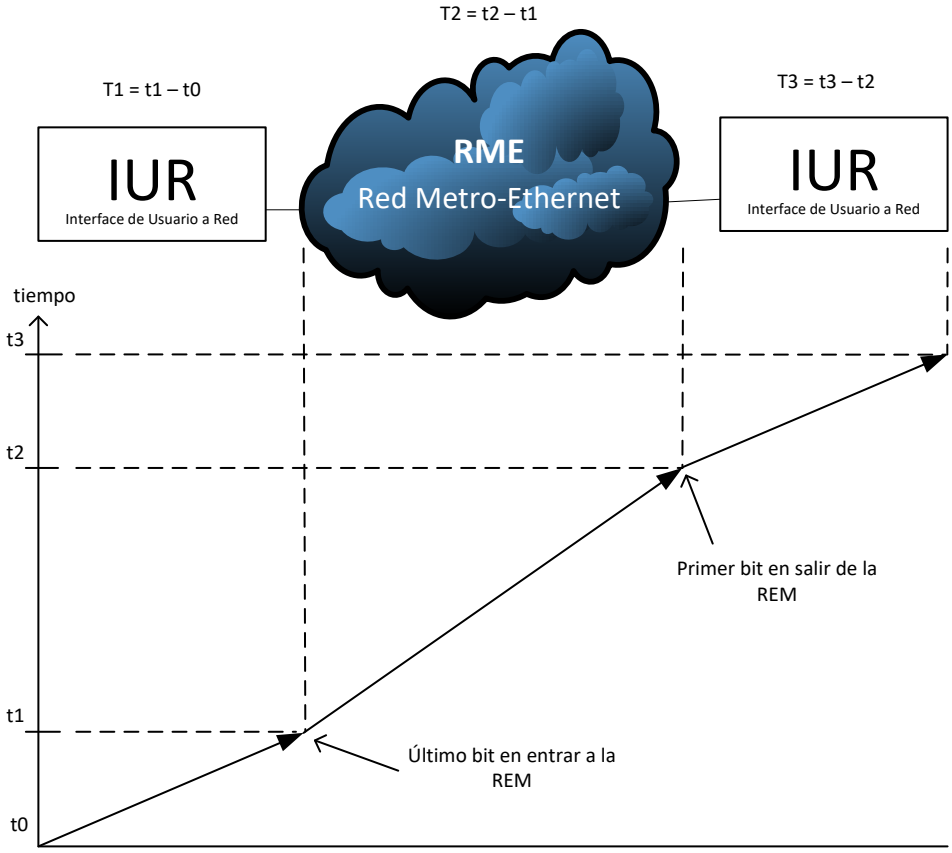
- Parámetros de desempeño Ethernet

Los parámetros de desempeño se refieren a aquellos que afectan de algún modo la calidad del servicio experimentada por el subscriptor. Estos parámetros de desempeño son los siguientes:

- Retraso de las tramas (*delay,* por su nombre en inglés)

El retraso de las tramas es un parámetro crítico de desempeño ya que puede tener un fuerte impacto en la calidad del servicio para aplicaciones en tiempo real tales como voz sobre IP; se refiere el retraso que pueden tener las tramas debido al tiempo que consume cada interface equipo o elemento de red, o red en general, desde el momento que recibe una trama y es capaz de despacharla hacia la ruta de destino. Para explicar este fenómeno se considera en la figura 4.

Figura 4. **División del retraso de las tramas en la red**



Fuente: elaboración propia.

En la figura 4 se identifican dos elementos que contribuyen al aumento del retraso de la transmisión de las tramas sobre la red: el primero se refiere al tiempo que le toma a la interface física del IUR tanto en el punto de partida como en el destino; el segundo que corresponde al tiempo que le toma a la RME desde el momento en que el último bit es entregado a la REM hasta que esta es capaz de egresar el primer bit hacia el IUR. En otras palabras, T1 y T3 será el tiempo que le tomas a las interfaces físicas de IUR y T2 el de la RME; la suma de estas tres es el retraso de las tramas total para comunicarse entre los dos IUR mostrados en la figura 4 es una característica estadística de las RME

del operador medida sobre un intervalo de tiempo. A continuación, se representa de acuerdo a la figura 11 el retraso de las tramas.

$$Retraso\ de\ las\ tramas = T1 + T2 + T3$$

En donde T1 y T3 puede ser calculado con base en las características de las IUR y el tamaño de las tramas, mientras T2 es especificado sobre un intervalo de medición. El retraso de las tramas es definido como el valor máximo medido de retardo de las tramas de servicio sobre un intervalo de tiempo.

El parámetro retraso de las tramas en la red es utilizado como atributo en la definición de clase de servicio. El retraso de las tramas en la red es un parámetro crítico especialmente para las aplicaciones en tiempo real como telefonía IP.

Fluctuación de fase de trama (*jitter* por su nombre en inglés)

La fluctuación de fase de trama, también conocido como variación del retraso, en el resto de este escrito será empleado el término en inglés, *jitter*, por facilidad del lector.

La medición del *jitter* puede ser derivado de las mediciones propias del retraso de las tramas. Durante el proceso de población de las muestras que mostraron retraso en la transmisión de las tramas y que son utilizadas para el cálculo de retraso de las tramas se obtienen dos valores: el valor más alto de retraso de la trama de servicio que representa el retraso de las tramas, además, la muestra con valor más bajo en retraso de las tramas de servicio. La diferencia entre el valor máximo y el mínimo es la forma de calcular el *jitter*.

$$Jitter = Retraso\ de\ la\ trama_{(maximo)} - Retraso\ más\ bajo_{(\text{minimo})}$$

El *jitter* es al igual que el retraso de las tramas un parámetro crítico para las aplicaciones en tiempo real, aplicaciones que requieren un nivel bajo y limitado de *jitter* para funcionar apropiadamente. Mientras que para aplicaciones que no son en tiempo real, el *jitter* no tiene efectos negativos en la calidad de experiencia. El parámetro *jitter* en la red es utilizado como atributo en la definición de clase de servicio.

- Pérdida de tramas (*packet loss*)

La pérdida de tramas indica en forma porcentual la relación de tramas entregados satisfactoriamente contra la totalidad de las tramas enviadas entre IUR sobre un intervalo de medición. Dicha relación se calcula de la siguiente forma, a medida que la cantidad de tramas entregadas satisfactoriamente son iguales que la cantidad de tramas enviadas, la pérdida de tramas tiende a cero.

$$Pérdida\ de\ tramas = \left(1 - \frac{Número\ de\ tramas\ entregadas\ a\ la\ IUR\ destino}{Total\ de\ tramas\ enviadas\ a\ la\ IUR\ destino}\right) \text{x } 100$$

La pérdida de tramas tiene un diferente impacto sobre la calidad de servicio, dependiendo de la aplicación, o protocolo de capas superiores usados para el servicio. Por ejemplo, un 1 % de paquetes perdidos para una aplicación de voz sobre IP puede ser aceptable. Un 3 % de paquetes perdidos, sin embargo, podría dar por resultado que la calidad de voz sea inaceptable. Las aplicaciones de multimedia pueden soportar varios grados de pérdidas de paquetes, compensado por ajustes en la tasa de transmisiones como sea detectada la tasa de paquetes perdidos.

Aplicaciones basadas en TCP, tales como requerimientos de navegación a Internet HTTP pueden tolerar varios grados de paquetes perdidos porque el protocolo TCP retransmitirá los paquetes que sean detectados perdidos. Sin embargo, si se incrementan excesivamente los paquetes perdidos afectará negativamente la calidad de servicio del subscriptor. El parámetro de pérdida de tramas en la red es utilizado como atributo en la definición de clase de servicio.

1.6. Topología de una red metro-Ethernet

Para un red metro-Ethernet se pueden emplear las topologías que se conocen para muchas de las tecnologías de red, las cuales se refieren a la comunicación que se emplea para computadoras que intercambien información, es decir, a la forma en que se diseña la red, a nivel físico o lógico determinando únicamente la configuración de las conexiones entre los nodos que la conforman. Las interconexiones físicas, las tasas de transmisión y los tipos de señal no son de la incumbencia en la topología de red, aunque pueden verse afectadas.

- Topología punto a punto

Se basa en el concepto más básico de comunicación, que se compone de un medio de enlace entre punto A y punto B, o como su nombre lo indica punto a punto, el mismo que se emplea en la telefonía convencional.

- Topología en estrella

Se basa en un punto central o nodo que se encarga de la conexión de los dispositivos, los cuales no están conectados entre sí, por lo cual la transmisión de datos es transferida por el nodo central. Su nombre se deriva de la forma

que suele tener en forma de estrella. Este tipo de topología es muy utilizada en redes de área local.

- Topología en árbol

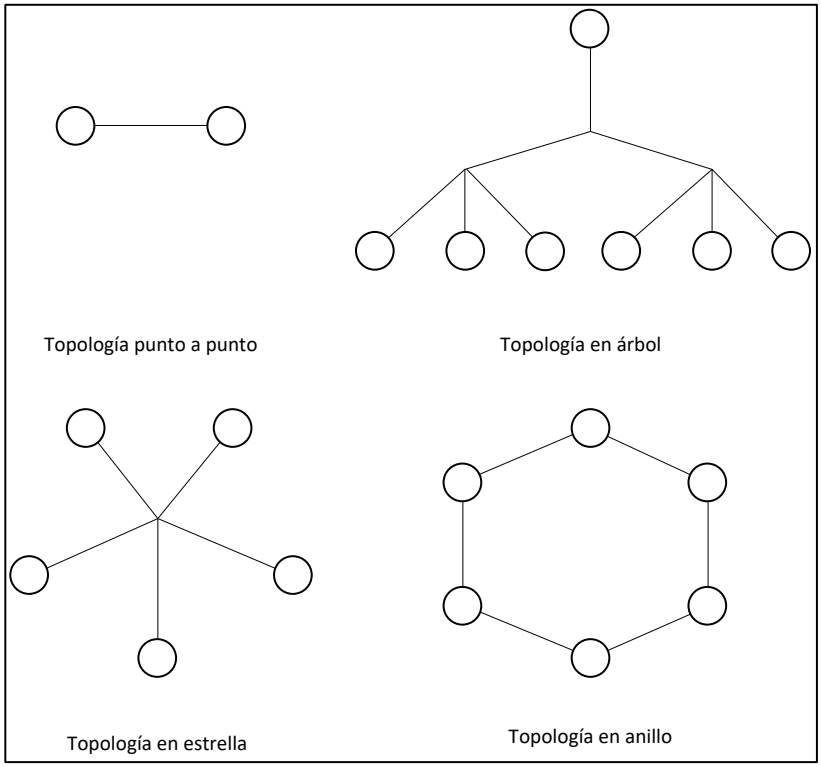
También conocida como topología jerárquica, denominación que se le otorga por su forma parecida a un árbol o diagrama de jerarquía está conformada por topologías en estrella, aunque difiere en el hecho de que no tiene un nodo central. Sin embargo, si posee un nodo de enlace troncal, que generalmente es un *hub* o *switch*, desde el que se ramifican los demás nodos.

- Topología en anillo

La topología en anillo definido así por su forma y porque todos los elementos que lo componen son accesibles desde cualquier otro elemento del anillo por dos rutas; brindan el respaldo de la transmisión de los datos ante la falla de uno de los tramos de comunicación entre dos elementos del anillo.

En la figura 5 se muestran, en resumen, las formas básicas de cada una de las topologías descritas anteriormente.

Figura 5. **Topologías de red**



Fuente: elaboración propia.

La topología en anillo presenta un escenario particular por consistir de un circuito cerrado; con el fin de ofrecer redundancia y respaldo a los circuitos de comunicación, es necesaria la ayuda de protocolos de red que contribuyan en tres funciones a topologías en anillo:

- Evitar *loops*

Los bucles, o *loops* por su nombre en inglés, suceden cuando todos los nodos del anillo poseen información de un camino para alcanzar su destino por alguno de sus vecinos y continúan entregándolo a sus vecinos creyendo que

este podrá entregarlo al destinatario; conlleva a que la información nunca alcanza su destino y se queda en un ciclo repetitivo.

La creación de un *loop* en una red produce el reenvío de información de forma indefinida, el consumo de ancho de banda de la red y procesamiento de los dispositivos; dan como resultado la degradación de los servicios en la red, en muy poco tiempo, y de continuar, hasta el colapso de la red.

- Selección de caminos alternos

Definir caminos alternos para cualquier destino ante una falla del camino o ruta principal, es decir, este tipo de protocolos apoyará la selección de la o las rutas de respaldo.

- Selección ruta única

Asegurar que exista solo una ruta de comunicación entre cualquiera de dos nodos. Es decir, estos protocolos brindarán a topologías en anillo el equilibrio entre circuitos de comunicación con rutas de redundancia, que evitan que se creen *loops* y asegurando un camino de comunicación.

En los próximos capítulos se estudiarán los protocolos de red que brindan estas funciones para una topología en anillo y que serán parte de este estudio.

2. STP (*SPANNING TREE PROTOCOL*) Y RSTP (*RAPID SPANNING TREE PROTOCOL*)

Dentro de los protocolos diseñados para evitar *loops* y que a la vez permita seleccionar de forma automática caminos alternos ante la falla de una ruta principal existe el *spanning tree protocol,* o STP por sus siglas en inglés y una variación de este llamado *rapid spanning tree protocol,* o RSTP por sus siglas en inglés.

2.1. STP

Spanning tree protocol, o STP, es un protocolo de red operando sobre la capa de enlace del modelo OSI que permite a redes en anillo evitar *loops*, a la vez, que administra de forma automática las rutas o caminos alternos para alcanzar un destino; ofrece mayor fiabilidad a la red por medio de redundancia de sus rutas de transmisión ante la falla de una de estas rutas. Esto lo hace por medio de cálculos que realiza STP para establecer en la red enlaces únicos libre de *loops* entre los dispositivos de red, pero manteniendo los enlaces alternos desactivados como reserva, con el fin de activarlos en caso de fallo. El cálculo para establecer los enlaces principales ocurre cada vez que un enlace en la red presenta un cambio de estado.

2.1.1. Modo de operación de STP

STP es un protocolo que basa sus cálculos en prioridades y costos para determinar que ruta o camino seleccionar en todo momento; cuando ocurre algún evento, la prioridad y el costo se vuelven a calcular. La prioridad y el

costo se establecen con base en la prioridad y costos de los *switches* y de los puertos respectivamente.

STP realiza un cambio de topología a nivel lógico administrando los caminos de comunicación entre cada punto, pasando de una topología tipo anillo a una topología tipo árbol, la cual es libre de *loops*. Al definir la topología en árbol, también determina cada camino de menor costo hacia los nodos, expandiéndose hasta definir el camino para cada uno de los nodos que lo integran; a esto se debe el nombre árbol de expansión o *spanning tree,* por sus siglas en inglés.

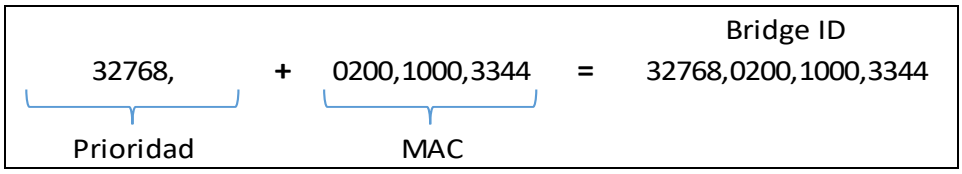
STP no siempre creará una topología *spanning tree* de menor costo, ya que un administrador de red puede alterar, si es necesario, algunos parámetros de configuración de tal forma que afecte la selección de la topología y con esto se afectaría que el costo de todos los caminos.

Dentro de STP existen algunos conceptos básicos que son definidos a continuación y que ayudarán a entender cómo el protocolo establece el árbol de expansión ante cualquier evento.

2.1.2. *Root bridge*

La primera tarea que debe atender el protocolo STP al iniciarse es seleccionar el *root bridge,* o RB por sus siglas en inglés. Esto lo realiza basado en el *bridge* ID o BID, el *switch* con menor BID es seleccionado como RB. Cada *switch* posee un número de prioridad del *switch* configurable y una dirección MAC; el BID está compuesto por la combinación de prioridad del *switch* + MAC; ver figura 6 para conocer un ejemplo de la definición del *bridge* ID:

Figura 6. **Definición de *bridge* ID**



Fuente: elaboración propia.

El valor predeterminado para prioridad del *switch* es 32768 y solo puede ser configurado en múltiplos de 4096. Durante el proceso de selección del RB, se compara primero la prioridad de *switch* de todos y se emplea la MAC si las prioridades son iguales; y el RB será el que tenga el BID menor.

2.1.3. Determinar caminos de bajo costo

Cada interface tiene un parámetro configurable *span path cost* que es inversamente proporcional a la velocidad de transmisión y recepción que la interface puede soportar; es decir, a medida que la velocidad de las interfaces ha aumentado, su costo disminuye. En la tabla III se muestra la definición del costo en STP y su relación con la velocidad de las interfaces.

Tabla X. **Costo en STP basado en velocidad de las interfaces**

Velocidad interface	Costo en STP
4 Mbit/s	250
10 Mbit/s	100
16 Mbit/s	62
100 Mbit/s	19
1 Gbit/s	4
2 Gbit/s	3
10 Gbit/s	2

Fuente: elaboración propia.

Cuando el *spanning tree* fue completamente calculado, este tiene la propiedad que cualquier mensaje entre un dispositivo y el RB atravesará el camino con menor costo; es decir, de todas las alternativas que existan entre el dispositivo y el RB el camino que atraviese será el de menor costo. El costo de atravesar un camino es la suma de los costos de los segmentos en el camino de acceso.

La propiedad de atravesar un camino de costo mínimo se basa en las siguientes dos definiciones:

- La selección del *root port*
- La selección del *designed port*

2.1.4. *Root port*

Luego de completar el proceso de selección del *root bridge*, se inicia la selección del *root port* o RP por sus siglas en inglés. Cada *switch* diferente al RB, deberá determinar por cual puerto conoce el camino con menor costo hacia

el RB; este será su RP del *switch*. Existirá por tanto en cada *switch* un RP, excepto en el RB.

2.1.5. *Designed port*

Con el RB seleccionado y RP determinado en cada *switch*, es necesario determinar porque puerto será conocido cada segmento de red; este es conocido como *designed port* para cada segmento de red, o DP por sus siglas en inglés, es decir, los *switches* en un segmento de red colectivamente determinan que *switch* tiene el camino con el menor costo desde el segmento de red hasta el RB. El puerto de la conexión de este *switch* para el segmento de red es entonces el DP para el segmento de red.

2.1.6. BPDU (*bridge protocol data units*)

STP intercambia mensajes de configuración llamados *bridge protocol data units,* o BPDU por sus siglas en inglés, los cuales son empleados por los *switches* para comunicarse entre sí; estos mensajes contienen información acerca de los puertos, los *switchs*, las direcciones de prioridad de puerto. Los BPDU son intercambiados entre los *switchs* cada dos segundos como valor predeterminado con el fin de identificar cambios en la red y modificar el estado de puertos como sea requerido.

Cuando un *switch* se enciende, supone que es el RB y envía las BPDU que contienen la dirección MAC de sí mismo tanto en el BID raíz como emisor. Cada *switch* reemplaza los BID de raíz más alta por BID de raíz más baja en las BPDU que se envían. Todos los *switches* reciben las BPDU y así determinan que *switch* será el RB. Durante este período de intercambio de BPDU, la red STP no inicia de inmediato el envío de información, y sucede una serie cambios

de estados mientras se procesan los BPDU y se determina la topología de la red.

Los *topology change notification* o TCN BPDU son usados para informar a los demás *switches* de cambios. Los TCN se inyectan a la red mediante un *switch* que no es el RB y se propaga hacia el RB. Tras la recepción del TCN, el RB instala una bandera o *flag* de cambio de topología en su BPDU normal; esta bandera se propaga a todos los otros *switches* para que actualicen rápidamente sus entradas de la tabla de envíos.

2.1.7. Estados de puertos en STP

- *Blocking*

Un puerto que causaría un loop en la red se pone en modo *blocking* o bloqueado. No hay envío o recepción de datos de usuario sobre un puerto en modo *blocking*, pero puede cambiar de estado de acuerdo a cambios sobre la red, y si el RB determina que el puerto debe cambiar de estado. Aún en este estado los menajes BPDU se continúan enviando o recibiendo.

- *Forwarding*

El puerto recibe y envía datos en su modo *forwarding* o de reenvío. STP mantiene monitoreados en los BPDU de entrada si un cambio ocurre sobre el puerto, y se debe actuar cambiando a modo *blocking* para evitar un *loop* en la red.

Todos aquellos puertos que no son RP o DP automáticamente el STP los pone en modo *blocking* y aquellos RP o DP los pone en modo *forwarding*.

- *Listening*

Durante el proceso de los BPDU ante el cambio en un puerto, los *switches* lo pone en modo *listening* y esperan de una posible nueva información que pueda causar que este regrese a modo *blocking*. Este estado no es poblado en la tabla de direcciones MAC y en este estado el puerto no reenvía tramas.

- *Learning*

Durante el proceso en el cual los puertos aún no están enviando tramas, este empieza a aprender direcciones fuentes de las tramas recibidas y las empieza a agregar a la base de datos del *switch* de forma filtrada. Es decir, que por medio de este estado se alimenta la tabla de direcciones MAC, pero aún en este estado no son enviadas las tramas.

Cuando una computadora, un servidor o un dispositivo se conecta a la red el puerto donde se conecta se pone en modo *forwarding* hasta después de aproximadamente 30 segundos, cuando el puerto haya atravesado los estados previos como *listening* y *learning*.

- *Disabled*

No es estrictamente parte de STP. Un administrador es quien decide poner un puerto en estado *disable* de forma manual. En este modo de operación no existe envío o recepción de datos de usuario y STP no puede realizar cambios a este estado.

2.1.8. Temporizadores en STP

STP opera empleando tres temporizadores, o *timers*, por medio de los cuales determina la correcta convergencia ante una falla, o bien la presencia de un *loop* cuando ocurra un cambio en la red.

- *Hello time*

Este temporizador corresponde al tiempo que transcurre entre cada mensaje de BPDU de configuración que envía el RB. Este tiempo determina la frecuencia con la que los *switch* que no son RB intercambian los mensajes de BPDU, ya que estos reenvían los BPDU que reciben del RB. Los *switches* que no son RB, tienen un *hello time* que se usa para temporizar los BPDU TCN (*topology change notifications*). El valor predeterminado de un *hello time* es de 2 segundos.

- *Forward delay*

El tiempo que toma en los estados *listening* y *learning* es determinado por un valor conocido *forward delay* o retraso de reenvío (el valor predeterminado es 15 segundos y es definido por el RB). Sin embargo, si en un puerto se conecta un *switch*, el puerto puede mantenerse en modo *blocking* si se determina que al conectarse un *loop* podría aparecer en la red.

- *Max age*

STP almacena la mejor copia de BPDU que ha recibido hasta que deja de recibir las BPDU durante el período de tiempo especificado por *max age*. Este intervalo entonces es el tiempo máximo que un *switch* almacena una BPDU

antes de descartarla. Cuando el *max age* se alcanza, se asume un cambio de topología y elimina el BPDU almacenado. El valor predeterminado para este temporizador es de 20 segundos.

Para reducir el tiempo en el cual una red operando con STP pueda realizar cambios y establecer un nuevo árbol de expansión, cuando servidores o computadoras se conectan, o existen cambios en la topología, *rapid* STP fue desarrollado. A continuación, se describen los conceptos más importantes de *rapid* STP.

2.2. RSTP

El Instituto de Ingenieros Eléctricos y Electrónicos o IEEE (Institute of Electrical and Electronics Engineers) introdujo el *rapid spanning tree protocol,* o RSTP, como una evolución de STP, mejoró principalmente aspectos como el tiempo de respuesta a un cambio de topología, de 30 o 50 segundos en STP a aproximadamente 5 a 6 segundos (correspondientes a 3 *hello time*) con RSTP. El nombrado *hello time* es un importante y configurable intervalo de tiempo que es usado por RSTP para varios propósitos, su valor predeterminado es de 2 segundos.

RSTP logró estos cambios significativos introduciendo nuevos comportamientos durante los procesos de convergencia, nuevos roles para los puertos y una reducción en los estados, pasando de cinco a tres, con el fin de agilizar la convergencia de los enlaces luego de algún evento. Además, fue diseñado para ser compatible con su antecesor el STP por lo cual el modo de operación en muchos aspectos continúo siendo muy similar a STP.

2.2.1. Estados de los puertos en RSTP

La definición de los estados de los puertos en RSTP ahora se basa en lo que el puerto hace con las tramas entrantes.

- *Discarding*

Las tramas de usuarios no son reenviadas y además la tabla de direcciones MAC no se actualiza con las que son aprendidas por el puerto en este estado. El estado *discarding* se podría decir, buscando una analogía al STP, combina los estados *disabled*, *blocking* y *listening* de los estados de STP. El estado *Listening* no se requiere en RSTP porque este puede negociar rápidamente un cambio de estado.

- *Learning*

Este estado no sufrió modificaciones con respecto a lo definido en STP, en este estado no son reenviadas las tramas pero las direcciones MAC son aprendidas ya que se agregan a la tabla de direcciones MAC.

- *Forwarding*

Este estado se maneja de forma similar a lo definido en STP; un puerto en estado *forwarding* es completamente operativo, envía y recibe datos de usuarios.

2.2.2. Roles de puertos en RSTP

Considerando que para RSTP el RB se selecciona de la misma forma como se describió para el STP, identificando el BID menor.

- *Root port*

El *root port,* o RP, opera de forma idéntica al de STP, en el cual cada *switch* identifica el puerto por el cual tiene acceso al camino con menor costo hacia el RB, todos los *switchs* excepto el RB.

- *Designated port*

Tanto para STP y RSTP, el *designated port* se define de forma idéntica. Los *switchs* en un segmento de red en conjunto determinan cual *switch* tiene el camino de menor costo desde el segmento de red hasta el RB, y el puerto de este *switch* que conecta este segmento de red es el *designated port* o DP.

- *Alternate port*

El *alternate port,* o AP, es otro camino alterno hacia el RB diferente al usado por el RP.

- *Backup port*

El *backup port,* o BP, es un camino de respaldo o redundancia hacia un segmento de red por otro puerto que conecta a dicho segmento, diferente al usado por el DP.

- *Disabled port*

El *disabled port* tiene definición y operación idéntica al igual que la de STP. No es de uso estricto en STP y puede ser modificado manualmente por el administrador.

2.2.3. Tipos de conexiones en RSTP

Con el fin de volver más rápida la convergencia con RSTP, además de los roles, fueron definidos algunos tipos de conexiones para clasificar aquellos puertos que se saben que no es necesario actualizar un cambio de su estado y que consecuentemente puede ser manejado de forma diferente.

- *Edge port*

Un puerto puede ser configurado como *edge port* o EP si ellos son considerados puertos de acceso; no se empleará para conectar otro *switch*. Estos puertos EP pasan directamente a estado *forwarding*. Con RSTP continuará el monitoreo del puerto por BPDU en caso que un *switch* sea conectado a uno de estos puertos; además, RSTP puede ser configurado para detectar automáticamente EP. Tan pronto como el *switch* detecta una BPDU llegar a un EP el puerto se convierte en un puerto no EP.

- *Link-type*

RSTP llama la conexión entre dos o más *switches* como una conexión *link-type*.

- *Point-to-point link y shared port*

Un puerto que opera en modo *full-duplex* se asume que es una conexión *point-to-point link*, mientras que un puerto que opere en *half-duplex* (por medio de un *hub*) es considerado un *shared port* predeterminadamente en RSTP. Este tipo de ajuste automático puede ser anulado por la configuración explícita de un administrador.

RSTP mejora la convergencia en los enlaces punto a punto mediante la reducción del tiempo *max-age* a tres veces el *hello time*, además, la eliminación del estado *listening* e intercambiarlo por un poco de confianza, o por decirlo de otra forma, un apretón de manos entre dos *switchs* para lograr así la transición rápida del puerto a estado *forwarding*. RSTP no hace nada diferente a STP en los enlaces compartidos.

2.2.4. Diferencias en los BPDU de STP y RSTP

A diferencia de STP, en RSTP se responderán a las BPDU enviadas desde la dirección del RB (*root bridge*). Un switch diferente al RB, en RSTP, podrá proponer su información de *spanning tree* de sus DP (*designed port*). Si otro *switch* RSTP recibe esta información y determina que es la superior información de raíz, este establece todos sus otros puertos en *discarding*. El *switch* puede enviar un mensaje de aceptación hacia el primer switch confirmando su superior información de *spanning tree*. El primer *switch*, al conocer la recepción de este acuerdo, sabe que puede pasar rápidamente al puerto en estado *forwarding* sin pasar por la transición de los estados *listening* y *learning*. Esto esencialmente crea un efecto en cascada lejos del RB donde cada *switch* propone a sus vecinos para determinar si esto puede hacer una

rápida transición. Esto es uno de los principales elementos que permiten a RSTP lograr tiempos de convergencia más rápido que STP.

Como se discutió en los detalles de rol de puertos anteriormente, RSTP introduce dos nuevos roles para mantener una copia sobre caminos alternos para el RP y el DP; esto evita tiempos de espera en caso que un desvío de los puertos actuales en producción fallara o que un BPDU no se recibiera en el RP o se demorará durante un intervalo.

2.3. Múltiple STP

El *multiple spanning tree protocol* es una extensión de RSTP y STP para desarrollar aún más la utilidad de las redes de área local virtuales (VLAN). MSTP configura un árbol de expansión (*spanning tree*) independiente para cada grupo de VLAN y bloquea todos menos uno de los posibles caminos alternativos dentro de cada árbol de expansión. Si solo hay una VLAN en la red, el tradicional STP funcionaría adecuadamente, pero si la red contiene más de una VLAN, la red lógica configurada por solo STP funcionaría, pero es posible hacer un mejor uso de los caminos alternativos disponibles mediante el uso de un árbol de expansión alternativo para diferentes VLAN o grupos de VLAN.

2.4. Tiempos de convergencia en STP y RSTP

Considérese el escenario donde presenta la caída de uno de los enlaces del anillo corriendo STP; la falla puede ser detectada de dos formas: mediante la detección de pérdida de señal a nivel físico, o por la pérdida del mensaje BPDU después de pasado el tiempo de espera en que este mensaje debe llegar y que la falla a nivel físico no fue detectada.

El proceso de convergencia tomará 2 veces el *forward delay*, en caso de que la falla es detectada, serán 2 veces uno para pasar por los estados *listening* y *learning*. Si la falla ocurre y la falla no es detectada es necesario que el mensaje BPDU expire en cada *switch* siendo esto en cualquier momento:

$$Tiempo\_Converger = \left(Max_{Age} - Message_{Age}\right) + 2\ x\ ForwardDelay$$

Donde:

- *Max_age* es el tiempo máximo que un *switch* almacena una BPDU antes de descartarla, antes de asumir un cambio de topología.

- *Message_age* se refiere al tiempo transcurrido desde que el mensaje fue generado.

Por tanto, el tiempo máximo para converger es cuando este es cero, así:

$$Tiempo\_Converger = Hello\_Time\ + Max_{Age} + 2\ x\ ForwardDelay$$

Tanto *hello_time*, *max_age* y *forward_delay* pueden ser configurados, hasta que *tiempo_converger* llegue a ser el mínimo posible; pero podría ocasionar que ante posibles cambios de topología un *loop* aparezca, o que se retrase un mensaje BPDU y se inicie un proceso de cambio de topología, cuando realmente no lo existe. Algunos fabricantes de elementos de red que operan con este protocolo, detallan los márgenes bajo los cuales se pueden variar estos temporizadores:

- *Max_age* tendrá por valor predeterminado 20 segundos, pero puede configurarse entre 6 y 40 segundos.

- *Forward_delay* tendrá por valor predeterminado 15 segundos, pero puede configurarse entre 4 y 30 segundos.

A medida que estos temporizadores sean configurados hasta sus valores más bajos el riesgo que un *loop* aparezca en la red aumenta y no sea detectado a tiempo o una posible degradación del servicio. Por tanto, si se consideran los tiempos de valores predeterminados por el protocolo STP, el tiempo de convergencia será hasta de 50 segundos.

En lo que corresponde a RSTP el tiempo de convergencia, hay que recordar que el principal objetivo de RSTP es reducir este tiempo en comparación con STP; por tanto, se analizará como RSTP lo ejecuta. Con solo asumir que los puertos durante una transición pasan un estado de reenvío de paquetes de una forma relativamente rápida, simplemente incrementando la velocidad de envejecimiento de las direcciones MAC no es suficiente.

Entonces, cuando un cambio de topología es detectado, RSTP envía instrucciones a los *switches* para que actualicen completamente su tabla de direcciones MAC. Con Ethernet, resulta que este proceso es fluido y sin restricciones hasta el momento cuando todas las direcciones MAC son nuevamente aprendidas. Como se mencionó anteriormente, cuando el *switch* que detecta un cambio de topología envía un BPDU con una bandera activa (*topology change* TC) hasta el *root bridge* (RB).

Los BPDU con la bandera TC activa tiene una duración en segundos de:

$$TC\ (duración) = 3\ x\ HelloTime$$

Según algunos fabricantes de elementos de red que operan con este protocolo, muestran que para el temporizador *hello time* emplea como valor predeterminado de dos segundos. Por tanto, en RSTP el tiempo de convergencia se ve significativamente disminuido a 6 segundos, con los valores predeterminados, en comparación con STP con 50 segundos. Si se busca reducir el tiempo de convergencia los puertos podrían operar en modo *portfast* y operar en modo *full-duplex* para reducir en RSTP hasta aproximadamente unos 400 a 600 milisegundos.

3. EAPS (*ETHERNET AUTOMATIC PROTECTION SWITCHING*)

Dentro de los protocolos que sirven para evitar *loops* y que a la vez permita la convergencia de los circuitos también existe el *Ethernet automatic protection switching,* o EAPS por sus siglas en inglés.

El protocolo EAPS fue inventado por Extreme Networks para mejorar la disponibilidad de los enlaces o circuitos de los clientes y permitir a los operadores tener una red más robusta; y así buscan alternativas para minimizar los tiempos de recuperación ante una falla como en uno de los caminos en una topología en anillo.

EAPS trabaja en topologías anillo para redes metro-Ethernet (RME) o redes de área local (LAN).

3.1. Modo de operación

El protocolo EAPS es un esquema lineal de protección diseñado para proteger VLAN basado en redes Ethernet. Los operadores manejan el tráfico de sus clientes de forma independiente, y lo hacen separándolos a nivel lógico empleando el método de *virtual local area network* o VLAN.

El protocolo EAPS opera bajo el concepto de dominios, y un único dominio EAPS existe en un solo anillo Ethernet, y sobre este dominio existen los segmentos de red que puedan comunicarse entre sí. Cualquier VLAN que sea

necesario proteger debe ser configurada sobre todos los puertos en el anillo para el dominio de EAPS determinado.

En el protocolo EAPS un dominio protegido es configurado con 2 caminos o *Path* del inglés, uno de estos es *working path* o camino en producción y el otro el *protection path* o camino de protección. Normalmente el tráfico de los subscriptores es transportado por el *working path*, con esto el *working path* se vuelve activo, y el *protection path* se vuelve inactivo. Si el *working path* falla, EAPS intercambia el tráfico de los subscriptores hacia el *protection path* y este último pasa a estar en modo activo.

Cada dominio EAPS tiene en la topología anillo un único *switch* designado como *master node* o MN, que es seleccionado manualmente por el administrador de la red durante la configuración. El resto de los *switches* que conforman el anillo son llamados como *transit nodes* o TN, al crear el dominio EAPS, definiendo los *switches* que lo conformarán y seleccionar el MN los demás *switches* se identifican a sí mismos como TN.

Recuérdese que cada *switch* tendrá, por estar en una topología en anillo, dos puertos conectados al anillo. Uno de estos puertos del MN será el *primary port* o PP hacia el anillo, y el otro será designado como *secondary port* o SP. Ambas designaciones PP y SP también son definidas por el administrador de forma manual.

En operación normal el MN bloquea el SP para todas aquellas tramas diferentes a las tramas de control Ethernet perteneciente al dominio EAPS determinado; es decir, principalmente el tráfico de los subscriptores que evitan así que se cree un *loop* en la red.

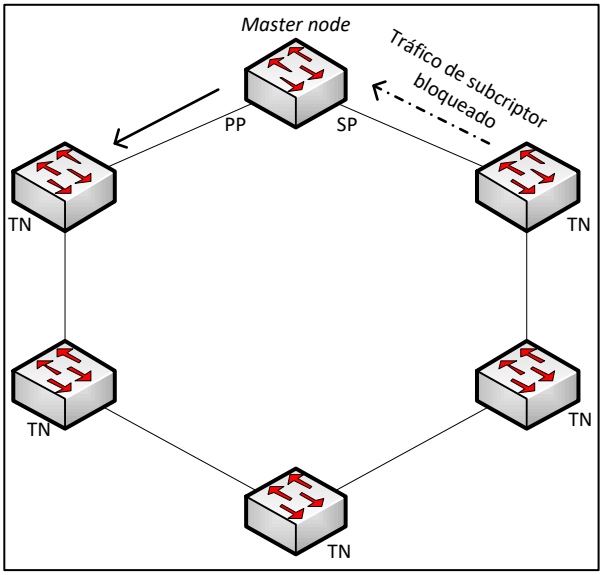
En EAPS existen mecanismos Ethernet para la conmutación y aprendizaje que operan según las normas existentes en este anillo. Esto es posible porque el MN hace parecer el anillo como una red libre de *loop* desde la perspectiva Ethernet.

Si el MN detecta una falla en el anillo, este cambia el estado del SP poniendo en modo activo, y permite así que las tramas fluyan por medio de este puerto. EAPS además emplea un control VLAN o VLAN de control por la que intercambia las tramas de control con información de alertas y sondeos de estados de las conexiones que conforman el anillo. Este control VLAN puede pasar siempre a través de todos los puertos en el dominio EAPS, incluyendo el SP del MN.

EAPS usa una combinación de mecanismos, uno de revisión constante o *polling* y otro de notificación o *alert*, para verificar la conectividad del anillo y determinar rápidamente una falla.

En la figura 7 se muestra una topología en anillo operando con el protocolo EAPS en el modo de operación normal. En el cual se resaltan el *master node*, los *transit nodes* (TN) y el *primary port* y *secondary port*. Una línea punteada que viaja hacia el SP resalta que únicamente el tráfico de control es permitido y el tráfico de subscriptor es bloqueado.

Figura 7. **EAPS en modo de operación normal**



Fuente: elaboración propia.

3.1.1. Alerta enlace caído (*link down alert*)

Cuando un TN (*transit node*) detecta un enlace caído sobre alguno de sus puertos en el dominio EAPS, el TN inmediatamente envía una trama de control de *link down alert* sobre el control VLAN hacia el MN.

Cuando el MN recibe la trama de control con el *link down alert*, el MN mueve de su estado normal de operación hacia un estado de *ring-fault* o anillo con falla y desbloquea su SP (*secondary port*). Además, el MN vacía su *forwarding data base*, FDB o base de datos de reenvío, y envía una trama de control llamada *ring down flush FDB* o anillo caído vaciar FDB hacia los demás *switches* del anillo con instrucciones de vaciar sus FBD también.

Luego de que las FDB fueron vaciadas, cada nodo y el MN empiezan a aprender la nueva topología.

3.1.2. Sondeo del anillo (*ring polling*)

El MN envía una trama de control llamada *health-check* sobre el control VLAN con una frecuencia configurable por el administrador en un temporizador llamado *hello timer*. Si el anillo está en su operación normal, la trama de *health-check* es recibida en el SP del MN, completando así todos los *switches* intermedios que componen el anillo; cuando este ocurre el MN reiniciará un temporizador llamado *fail-timer* y continuará operando en modo normal.

Si el MN no recibe la trama de control *health-check* después del período definido por el *fail-timer*, el MN cambia del modo de operación normal hacia el estado *ring-fault* y desbloquea el SP. El MN además vacía su FDB y requiere por control VLAN que los demás *switches* del dominio EAPS realicen la misma operación vaciando sus FDB, enviando el mensaje *ring down flush FDB*. Luego de que los FDB fueron vaciados, cada nodo y el MN empiezan a aprender la nueva topología. Este mecanismo de *ring polling* es un método de respaldo al envío de las tramas de control *link down alert* por si acaso dicha trama se perdiera durante la transición hacia el MN.

3.1.3. Restauración del anillo (*ring restoration*)

El MN continúa enviando periódicamente la trama de control *health-check* por su PP incluso cuando entra en estado *ring-fault*. Una vez que el anillo se restaura, la siguiente trama de control *health-check* será recibida en el MN en el SP, esto causará que el MN inicie el proceso *ring restoration* o restauración del anillo.

El proceso de *ring restoration* se completará cuando el MN llegue a su modo de operación normal, e inicia bloqueando en el SP para todas aquellas tramas diferentes a las tramas de control Ethernet perteneciente al dominio EAPS determinado; es decir, principalmente el tráfico de los subscriptores, para evitar la aparición de un *loop*; además vaciará su FDB y requerirá por medio de una trama de control llamada *ring up flush FDB* que los TN del dominio EAPS lo realicen también; por último, se empezará a aprender la nueva topología.

Durante el tiempo entre la detección que un enlace se restauró por parte de un TN y que el MN detecta que el anillo fue restaurado, el SP del MN está aún abierto o enviando tramas de tráfico del subscriptor, creando la posibilidad de un *loop* temporal en la topología.

Para prevenir esto, el TN ejecutará las siguientes acciones:

- Pondrá todas las VLANs protegidas y que transitan por el puerto que recientemente se restauró en un estado de bloqueo temporal.

- Guardará en un registro local el identificador del puerto que ha sido bloqueado temporalmente.

- Y se pondrá en un estado llamado *pre-forwarding* de transición.

Con estas acciones sobre el TN que notificó la restauración del puerto, se evitará que un *loop* temporal se cree a lo largo de la red.

Cuando el TN que tiene el estado *pre-forwarding* reciba una trama de control del MN *ring up flush FDB*, el TN ejecutará las siguientes acciones:

- Ejecutará el vaciado de su FDB.

- Desbloqueará los puertos de las VLANs protegidas, que están guardados en su registro local y que fueron bloqueados temporalmente y por la reciente actualización de restauración.

- Y cambiará su estado de transición *pre-forwarding* a su estado normal de operación.

3.1.4. Múltiples dominios EAPS

Un *switch* que tiene EAPS habilitado puede ser parte de más de un anillo, por lo que un *switch* que tenga EAPS habilitado también puede pertenecer a más de un dominio EAPS al mismo tiempo. Cada dominio EAPS sobre un *switch* requiere una instancia independiente del protocolo EAPS sobre el mismo *switch*, y una instancia por anillo protegido EAPS.

También, se puede tener más de un dominio EAPS en ejecución sobre el mismo anillo al mismo tiempo. Cada dominio EAPS tiene su propio y único MN y su propio conjunto de VLANs protegidas. Esto facilita la reutilización de ancho de banda de los anillos.

3.2. Encabezado de EAPS

En la tabla XI se muestra como es la distribución de la trama EAPS y el tamaño de cada campo.

Tabla XI. **Formato de la trama EAPS**

<table>
<tr><th colspan="48">Formato Trama EAPS</th></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td><td>32</td><td>33</td><td>34</td><td>35</td><td>36</td><td>37</td><td>38</td><td>39</td><td>40</td><td>41</td><td>42</td><td>43</td><td>44</td><td>45</td><td>46</td><td>47</td></tr>
<tr><td colspan="48">Destination MAC Address (6 Bytes)</td></tr>
<tr><td colspan="48">Source MAC Address (6 Bytes)</td></tr>
<tr><td colspan="16">EtherType</td><td colspan="4">PRI</td><td colspan="12">VLAN ID</td><td colspan="16">Frame Length</td></tr>
<tr><td colspan="16">DSAP / SSAP</td><td colspan="8">CONTROL</td><td colspan="24">OUI = 0x00E02B</td></tr>
<tr><td colspan="16">0x00bb</td><td colspan="8">0x99</td><td colspan="8">0x0b</td><td colspan="16">EAPS_LENGTH</td></tr>
<tr><td colspan="8">EAPS_VER</td><td colspan="8">EAPSTYPE</td><td colspan="16">CTRL_VLAN_ID</td><td colspan="16">0x0000</td></tr>
<tr><td colspan="16">0x0000</td><td colspan="32">SYSTEM_MAC_ADDR (6 Bytes) ...</td></tr>
<tr><td colspan="16">... SYSTEM_MAC_ADDR (6 Bytes)</td><td colspan="16">HELLO_TIMER</td><td colspan="16">FAIL_TIMER</td></tr>
<tr><td colspan="8">STATE</td><td colspan="8">0x00</td><td colspan="16">HELLO_SEQ</td><td colspan="16">0x0000</td></tr>
<tr><td colspan="48">RESERVED (0x000000000000)</td></tr>
<tr><td colspan="48">RESERVED (0x000000000000)</td></tr>
<tr><td colspan="48">RESERVED (0x000000000000)</td></tr>
<tr><td colspan="48">RESERVED (0x000000000000)</td></tr>
<tr><td colspan="48">RESERVED (0x000000000000)</td></tr>
<tr><td colspan="48">RESERVED (0x000000000000)</td></tr>
</table>

Fuente: elaboración propia.

Donde:

- *Destination* MAC *address* y *source* MAC *address* (6 bytes cada uno): se refiere a la dirección MAC de destino y fuente. En EAPSv1 la dirección MAC destino siempre es 0x00e02b000004.

- PRI (4 bits): se refiere a la prioridad del mensaje. Contiene 3 bits que definen dicha prioridad y mantiene un bit reservado.

- *EtherType* (2 Bytes): se refiere al tipo de protocolo que está siendo encapsulado sobre la trama Ethernet. En EAPSv1 siempre es 0x8100, que indica que es una trama con VLAN.

- DSAP / SSAP (2 bytes): se refiere *al destination service access point* y al *source service access point* respectivamente. El D-SAP (8 bits) representa la dirección lógica de la entidad de la capa de red que ha creado el mensaje. Y el S-SAP (8 bits) representa la dirección lógica de

la entidad de la capa de red que intenta recibir el mensaje. En EAPSv1 siempre tienen un valor 0xAAAA.

- *Control* (1 byte): define el formato del paquete, es usado para portar alguna información de control para servicios auxiliares, en el caso de EAPSv1 siempre tiene un valor de 0x03.

- EAPS_*LENGTH* (2 bytes): define la longitud del encabezado EAPS, el cual en EAPSv1 es siempre 0x40, equivalente a 8 bytes, que corresponden a los que ocupan los encabezados EAPS_*LENGTH* (2 bytes) EAPS_VER (1 byte), EAPS_*TYPE* (1 byte), CTRL_VLAN_ID (2 bytes) y 2 Bytes más reservados.

- EAPS_VERS (1 byte): define la versión de EAPS que se emplea, en nuestro caso versión 1, por lo cual el valor es 0x0001.

- EAPS_*TYPE* (1 byte): define el tipo de mensaje EAPS que se está enviando, puede tomar diferentes valores de acuerdo a la función que se esté haciendo.

Valores para EAPS *type* (EAPS_TYPE):

  - *Health*= 5. Se emplea cuando se envía el *health-check*.

  - *Ring-up-flush*-FDB = 6. Se emplea cuando se requiere vaciar *bridging table* porque fue restablecido un enlace que estaba caído.

- *Ring-down-flush*-FDB = 7. Se emplea cuando se requiere vaciar *bridging table* porque se identificó que un enlace fallo luego que estaba activo.

- *Link-down* = 8. Se emplea cuando se envía el *link-down alert*.

- CTRL_VLAN_ID (2 bytes): Define el VLAN ID para el Control VLAN en uso.

- *SYSTEM*_MAC_ADDR (6 bytes): Es la dirección MAC del nodo que está enviando el mensaje.

- *HELLO_TIMER* (2 bytes): este valor se define en el *master node* y define la frecuencia con la que serán enviadas las tramas de control *health-check*.

- *FAIL_TIMER* (2 bytes): este valor se define en el *master node* y define el tiempo que el MN esperará que el *health-check* vuelva al MN por el SP, antes de declarar una falla en el anillo.

- *HELLO*_SEQ (2 bytes): es el número de secuencia de las tramas de control *health-check*.

- *STATE* (1 byte): es el valor numérico que representa el estado sobre enlaces y *switchs*, este valor es usado de acuerdo al tipo de mensaje EAPS que se envíe.

Valores para EAPS del campo STATE:

- *IDLE* = 0 – Indica que el *switch* aún no está operando sobre el dominio EAPS.

- *COMPLETE* = 1 – Indica que el *master node* está en modo normal de operación.

- *FAILED* = 2 – Indica que existe una falla con el *switch*.

- LINKS-UP = 3 – Indica que los enlaces compartidos están activos en una configuración multidominio de EAPS.

- *LINK-DOWN* = 4 – Indica que se identificó que un enlace que estaba activo se fue abajo.

- *PRE-FORWARDING* = 5 – Indica que un *switch transit node* identificó que un puerto que estaba caído levanto, y que bloqueo dicho puerto para evitar un *loop* temporal. Mantendrá este estado hasta que reciba la trama de control *ring up flush* FDB.

- Todos los demás valores son reservados.

3.3. Tiempos de convergencia en EAPS

En EAPS se emplea un mecanismo básico, como se explicó, para identificar una falla en el anillo, llamado *link down alert* y es empleada luego que un TN identifica una falla en sus conexiones; bajo este caso puede tomar menos de 50 milisegundos que la alerta llegue al MN y se inicie el proceso de restauración del anillo, de acuerdo a la información de uno de los fabricantes de elementos de red que operan con el protocolo EAPS, el fabricante Extreme.

Por tanto, en comparación con STP o RSTP, que ofrecen tiempos de convergencia en sus valores predeterminados de 50 y 6 segundos respectivamente, aunque si RSTP podría reducir su tiempo de convergencia como se mencionó entre 400 a 600 milisegundos. EAPS con sus 50 milisegundos es mucho más rápido y puede ofrecer con este tiempo de convergencia, para servicios multimedia.

4. ANALISIS DE LA FACTIBILIDAD TÉCNICA Y ECONÓMICA PARA LA MIGRACIÓN DE UNA RED METRO-ETHERNET EN STP A EAPS

Hasta el momento se han descrito tres protocolos: STP, RSTP y EAPS, que trabajan en la capa de enlace para que redes con topología en anillo puedan brindar respaldo y redundancia a los caminos de comunicación ante una falla a la vez que evitan los efectos degenerativos de los *loops*.

En la actualidad estos protocolos son utilizados e implementados por los operadores de telecomunicaciones en sus redes de comunicación y transporte, con el afán de brindar a sus clientes servicios de forma confiable y estable; dichos servicios como se ha mencionado pueden ser *real time* y *non real time*, estos últimos, ya que emplean métodos de corrección de errores y se basan en protocolos como TCP, son menos susceptibles ante una falla y el tiempo de restauración o espera luego que una red en topología anillo converge por rutas secundarias. Por el contrario, los servicios *real time* son mucho más sensibles a estas fluctuaciones o alteraciones de la red.

Como se mencionó en el capítulo 1, los códec más utilizados en VoIP son G.711, G.723.1 y G.729. En la tabla XII se muestra el ancho de banda necesario para la transmisión de cada uno de estos códec.

Tabla XII. **Ancho de banda por códec para VoIP**

Codec	Algoritmo utilizado	Flujo de banda
G.711	PCM (*pulse code modulation*)	64 Kbps
G.726	ADPCM (*adaptive differential pulse code modulation*)	16, 24, 32, 40 Kbps
G.728	LD-CELP (*low delay code excited linear prediction*)	16 Kbps
G.729	CS-ACELP (*conjugate structure algebraic CELP*)	8 Kbps
G.723.1	MP-MLQ (*multi-pulse maximum likelihood quantization*)	6,3 Kbps 5,3 Kbps
	ACELP (*algebraic code excited linear prediction*)	6,3 Kbps 5,3 Kbps

Fuente: elaboración propia.

Los códec han ido evolucionando buscando la reducción de ancho de banda que es necesario para transmitir las muestras de voz sobre las tramas. Pero al mismo tiempo se corre el riesgo que más información de la voz se pierda en un corto período de tiempo.

Entre el proceso de codificación y decodificación, las tramas tienen que fluir de un punto a otro por diferentes tipos de medio, en este caso, una red metro-Ethernet; pero eventualmente las tramas pueden perderse por congestión de red o corrupción de datos, entre otros ejemplos de posibles causas. Obviamente, la calidad de la voz se verá afectada a medida que aumenten las tramas de voz que se pierdan. Varios factores afectan la calidad de voz percibida por los usuarios cuando se transmite a través de una red de datos. Estos factores incluyen la compresión utilizada (códec), el porcentaje de pérdida de paquetes, los retardos debidos a diversas causas (algoritmos de compresión, tiempo de procesamiento, latencia de la red, etc.), el eco, las variaciones en la demora (*jitter*) y el tamaño de los paquetes.

Para el tráfico *real-time* como la voz, las retransmisiones no son prácticas ya que pueden ocasionar retardos adicionales; por tanto, las puntos extremos manejan la comunicación con muestras de voz pérdidas también, llamado a este fenómeno como *frame erasures*.

Para reducir el impacto de *frame erasures* los códec hacen uso de técnicas como PLC *packet loss concealment* que consiste de reproducir, durante los períodos de perdida de tramas, un buffer que almacena las últimas muestras de voz recibidas; si las tramas pérdidas son pocas esta técnica vuelve imperceptible la pérdida de las tramas.

4.1. Medición de la calidad de voz en redes IP

La calidad de servicio o QoS por sus siglas en inglés (*quality of service*) se refiere al rendimiento de la red desde el punto de vista técnico, y al cumplimiento con los requerimientos para las aplicaciones. La VoIP enfrenta problemáticas propias de las redes de datos, que se manifiestan como degradaciones en la calidad del servicio percibida por los usuarios, denominando a esta percepción como calidad de experiencia o QoE por sus siglas en inglés (*quality of experience*). Estas degradaciones pueden deberse por ejemplo a retardos en las tramas, *jitter* (diferencia de retardos) y pérdida de paquetes, entre otros factores, que fueron explicados en el capítulo 1.

En la medida que la VoIP sea parte de un servicio con un fuerte despliegue por un operador de telecomunicaciones, es muy importante la calidad del servicio en la voz y desarrollar métodos para medirla. Estos métodos de medición pueden ser subjetivos y objetivos.

Los métodos subjetivos de medida de la calidad de servicio se basan en conocer directamente la opinión de los usuarios. Típicamente, resultan en un promedio de opiniones. Y los métodos objetivos miden propiedades físicas de una red para prever o estimar el rendimiento percibido por los usuarios.

- Métodos subjetivos

La puntuación de opinión media o MOS por sus siglas en inglés (*mean opinion score*) es el promedio de la calificación de categoría absoluta o ACR por sus siglas en inglés (*absolute category rating*) medido de la opinión de un gran número de usuarios. El ACR es la forma de medir directamente, sin comparaciones, la calidad de audio; es decir, que a criterio del usuario se le pide que califique el audio con valores entre 1 y 5, siendo 5 excelente y 1 malo de forma directa; el promedio de estas calificaciones se determinó los valores del MOS.

Muchos de estos estudios subjetivos son caros, lentos y requieren de la participación de un gran número de suscriptores, además, depende de factores externos a la calidad del audio, como la cultura y la experiencia del usuario.

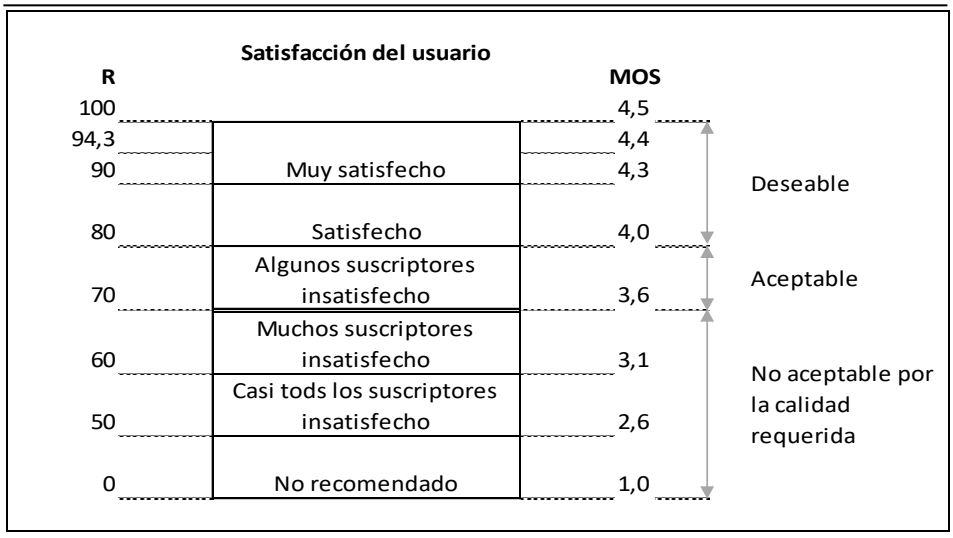
- Métodos objetivos

Para pasar de las mediciones subjetivas a valores objetivos, algunos estudios y pruebas relacionaron con varios parámetros de red medibles con los valores obtenidos de MOS. Dentro de estos métodos existe el modelo E recomendado por la ITU-T, como se había comentado (ITU Telecommunication Standardization Sector), es uno de los tres sectores o divisiones de la Unión Internacional de Telecomunicaciones o ITU (International Telecommunication Union).

El modelo E es un modelo informático que ha sido adoptado por varias organizaciones a nivel mundial ya que es el modelo más ampliamente difundido, el cual es una cuantificación escalar de la calidad de audio que se estima percibiría un usuario, con base en las pruebas realizadas y comparándolo contra la escala del MOS.

Una característica fundamental de este modelo es la utilización de factores de degradación de la transmisión que reflejen los efectos de los modernos dispositivos de procesamiento de señales. El modelo E se calcula, con base en varios parámetros medibles de la red, un parámetro R que puede relacionarse con el MOS de acuerdo a la figura 8.

Figura 8. **Relación entre escalas del modelo E y MOS**



Fuente: elaboración propia.

Los valores de R por debajo de 70, en la escala de MOS, serán considerados no aceptable. El valor R del modelo E se obtiene de la siguiente ecuación:

$$R = Ro - Is - Id - Ie + A$$

Donde:

- Ro se deriva del concepto básico de la relación señal a ruido, ruido referido al ambiente de donde se está originando la voz.

- Is relacionado con el volumen de la conexión y con la cuantificación.

Ambos (Ro como Is) son intrínsecos a la señal de la voz en la entrada de la red y no dependen de la red misma, al comparar VoIP a llamadas hechas sobre una red PSTN. No son influenciables desde cambios en la red.

- Id modela las degradaciones producidas por los retardos y el eco.

- Ie representa las degradaciones producidas por los códec y por las pérdidas de paquetes de distribución aleatoria.

- A factor de ventaja, que significa que el usuario está dispuesto a aceptar degradaciones en la calidad a cambio de facilidad de acceso (por ejemplo, en telefonía móvil o telefonía satelital).

En el modelo E el único factor que considera las degradaciones por pérdida de paquetes es el factor Ie; sin embargo, en una conversación telefónica realizada a través de VoIP, la tasa de pérdida de paquetes o tramas no puede considerarse constante, ya que es muy común que estas se presenten en forma de ráfagas por congestión en la red o corrupción de los datos y durante el resto del tiempo se mantenga en valores bajos. Por tanto, no

se puede asumir que la calidad de la voz es constante, dependerá de las condiciones de la red en el momento que sea evaluado.

Cuando se presentan estas ráfagas de pérdidas de paquetes hay que considerar que la percepción humana no varía en forma instantánea. Por tanto, se propone considerar un modelo exponencial para modelar la evolución de la percepción en función de los cambios instantáneos según las recomendaciones de ETSI (European Telecommunications Standards Institute).

A medida que la pérdida de paquetes aumenta, el valor de Ie aumentará y por consiguiente el de R, del modelo E, disminuirá. En el anexo I de este documento se encuentra información de ITU-T Recomendación G.113-200102, en donde se detallan los valores de Ie con respecto al valor porcentual de pérdida de paquetes y el códec utilizado; ver tabla XIII.

Tabla XIII. **Valores del factor de degradación de equipo Ie con respecto a pérdida de paquetes por códec utilizado**

	Codec			
Pérdida de Paquetes (%)	G.711 sin PLC	G.711 con PLC	G.723.1 (6.3 Kbps)	G.729A
0	0	0	15	11
1	25	5	19	15
2	35	7	24	19
3	45	10	27	23
4	- *	- *	32	26
5	55	30	- *	- *
16	- *	- *	55	49
20	- *	50	- *	- *

* En el reporte del ITU-T REC-G.113-200102 no había valores disponibles para estas condiciones.

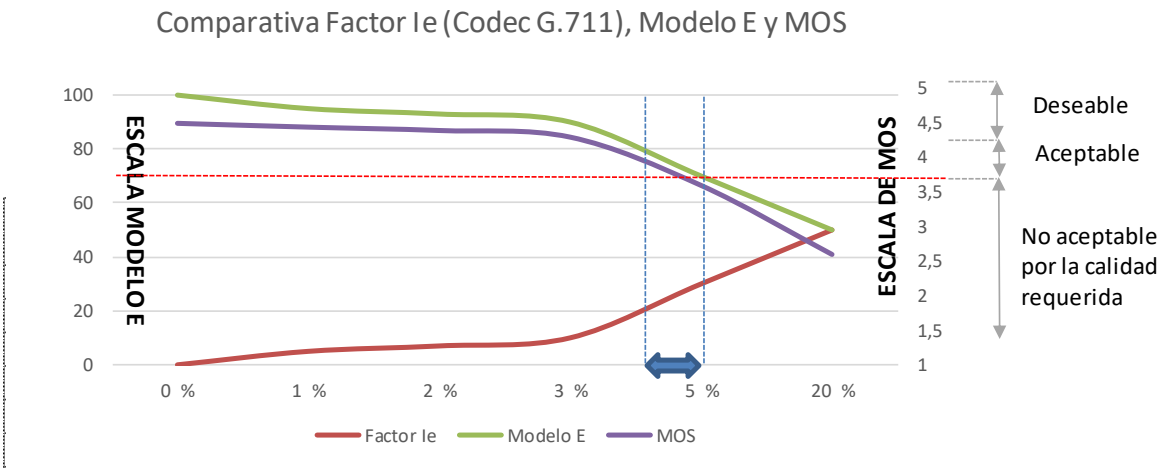
Fuente: elaboración propia.

Véase que cuando la tasa de pérdida de paquetes es 0 %, los códec G.723.1 y G.729A tiene un factor Ie de 11 y 15, respectivamente,

correspondiente al factor de degradación para Códec de velocidad baja. Además, observe como a medida que el porcentaje de las pérdidas aumenta en un 1 % el factor Ie aumenta exponencialmente.

Obsérvese que los únicos factores del modelo E, que contribuyen para que el valor R sea igual a 100, son Ro y A; valor en el cual R es equivalente a deseable o 4.5 en la escala MOS. Si se desprecia Is e Id y consideramos su Ie como único factor que hace que el valor de R disminuya se obtedrá la comparativa expuesta en la figura 9 con el caso específico del códec G.711.

Figura 9. **Comparativa factor ie (codec G.711), Modelo E (con factor Ie como único que disminuye R) y MOS**



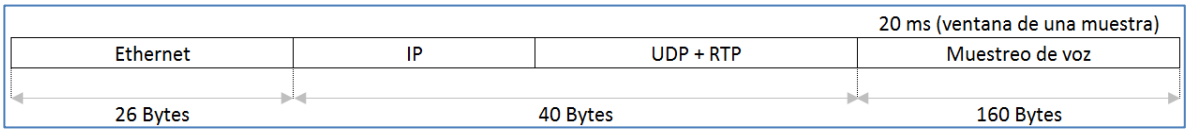
Fuente: elaboración propia.

Por tanto, de acuerdo a estos valores al alcanzar entre 4 % a 5 % de pérdida de paquetes durante el período de evaluación, el valor de R del modelo E llegará a valores menores a 70; como se explicó a un MOS categorizado como calidad de servicio no aceptable por la calidad requerida según la escala del modelo E, aun cuando los demás factores de degradación fueran 0. Esto

haría que servicios como la voz con mayores porcentajes de pérdida de tramas en la comunicación llegue a ser categorizada como una mala calidad de servicio.

Considérese el escenario de la transmisión de una trama empleando el Códec G.711 con una ventana de 20 ms y sabiendo que se tienen un flujo de datos para este códec de 64 kbps se obtienen 160 bytes para la trama VoIP, ver figura 16.

Figura 10. **Trama IP para códec G.711 y una ventana de 20ms**



Fuente: elaboración propia.

La tabla XIV muestra, entonces, el ancho de banda requerido en red para ser transmitido.

Tabla XIV. **Ancho de banda y cantidad de tramas por segundo por códec**

Tipo de Codec	Duración de trama (ms)	Bytes de voz/trama	Bytes de paquete IP	Bytes de trama Ethernet	Ancho de banda en LAN (Kbps)	Tramas por segundo
G.711 (64 kb/s)	10	80	120	146	116,8	100
	20	160	200	226	90,4	50
	30	240	280	306	81,6	33
G.729 (8 kb/s)	10	10	50	76	60,8	100
	20	20	60	86	34,4	50
	30	30	70	96	25,6	33
G.723 (6,3 kb/s)	20	16	56	82	32,7	50
	30	24	64	90	23,9	33
G.723 (5,3 kb/s)	20	13	53	79	31,7	50
	30	20	60	86	22,9	33

Fuente: elaboración propia.

En la tabla XIV se ha agregado la estimación de tramas por segundos que serían enviadas, de acuerdo a la ventana de tiempo por cada muestra; es decir si se considera una duración de trama de 10 ms, en un segundo se tendrán 100 tramas que deben ser enviadas. Este valor es importante para considerar si una falla se presenta en la red y se conoce el tiempo aproximado de recuperación estimado y si además se necesita mantener la calidad de servicio dentro de los valores aceptables.

En la tabla XV se muestra la cantidad de tramas que se podrían perder bajo tres escenarios de períodos de muestreo de 5, 10 y 15 segundos, considerando una tasa de pérdidas de paquetes del 4 %, ya que al aumentar este porcentaje el valor MOS caería en la categoría no aceptable por la calidad requerida.

Tabla XV. **Cantidad de tramas no entregadas al destino para alcanzar un 4 % de pérdidas de paquetes**

Tiempo de muestreo (seg)			5	10	15
Tiempo para 4 % pérdidas (ms)			200	400	600
Tipo de codec	Duración de trama (ms)	Tramas por segundo	Cant Tramas para 4 % pérdidas en 5 segs	Cant Tramas para 4 % pérdidas en 10 segs	Cant Tramas para 4 % pérdidas en 15 segs
G.711 (64 kb/s)	10	100	20	40	60
	20	50	10	20	30
	30	33	7	13	20
G.729 (8 kb/s)	10	100	20	40	60
	20	50	10	20	30
	30	33	7	13	20
G.723 (6.3 kb/s)	20	50	10	20	30
	30	33	7	13	20
G.723 (5.3 kb/s)	20	50	10	20	30
	30	33	7	13	20

Fuente: elaboración propia.

Por tanto, considerando el escenario de tiempo de muestreo medio de 10 segundos, ante una falla en una topología tipo anillo, la ruta alterna deberá ser conmutada en menos de 400 milisegundos, para evitar que el porcentaje de pérdidas de paquetes sea superior a un 4 %, que como se explicó, ubicaría la calidad en la escala de MOS como no aceptable por la calidad requerida.

4.2. Análisis y auditoría de la red actual en STP

Se propone para el estudio un operador que es proveedor de servicios de red, tanto *real-time* y *non real-time*, y aunque predominan los servicios *non real-time*, últimamente ha presentado una tendencia de crecimiento en lo que a contratación de servicios *real-time* se refiere.

Dicha red posee *switchs* Ethernet, empleando el protocolo TCP/IP, básicamente en capa dos, y operan con *spanning tree protocol* para la redundancia y evitar *loops* sobre la red que tiene una topología en anillo. Actualmente en la red propuesta los *switchs* implementados por el operador soportan tanto el protocolo STP como RSTP, pero no soportan el protocolo EAPS

Los nodos que componen la estructura de comunicación principal de la red están ubicados en el valle metropolitano, en sitios elegidos por cercanías a centros industriales y de oficina. La red del operador ha sido construida en una topología en anillo con el fin de brindar respaldo a los enlaces de comunicación, por lo que dicha red es considerada una red metro-Ethernet.

El operador ha comentado la necesidad de ampliar la capacidad de los switches, ya que requiere interfaces de mayor capacidad de transporte sobre los circuitos que compone el anillo, así como para tener una mayor de densidad

de puertos de acceso, esto último es mandatorio para cumplir con el crecimiento que proyecta el operador en clientes y servicios para los próximos años.

Considerando que es posible que el operador deba cambiar los equipos que componen el anillo ha pensado en que puede reutilizar algunos de los *switches* como parte de la red; algunas partes inventariarlas para reemplazo y el restante venderlo.

4.2.1. Descripción de los servicios

Los clientes del operador son primordialmente empresas medianas y grandes en relación a las operaciones que realiza y buscan intercambiar información con sus otras oficinas, bodegas y tiendas o en algunas ocasiones con proveedores o clientes; para lo cual el operador del estudio ofrece soluciones de enlaces de datos y servicios de telefonía IP o VoIP.

Existe un grupo en particular de clientes que son centros de atención al cliente, que además de adquirir grandes capacidades para servicios de telefonía IP, han ido en aumentado. El operador ha logrado atraer a varias de estas empresas como parte de sus clientes.

- Servicios de datos

Estos son los servicios que hemos descrito como *non real-time*, y el operador los ofrece como enlaces de datos de comunicación que el cliente requiere para enviar o recibir información entre sucursales o puntos de interés del cliente.

El operador diferencia los servicios de datos que provee por la velocidad con los siguientes valores 1 Mbps, 3 Mbps y 5 Mbps. Y así corresponde el precio de venta de estos servicios.

Aunque algunos de estos servicios de comunicación entre dos puntos que el cliente requiere, también se provee acceso hacia internet, y para el estudio se considera ambos tipos de conexión se maneja de igual forma, así como se tiene el mismo precio para ambos.

- Servicios de telefonía IP o VoIP

Estos son los servicios que se han descrito como *real-time*, y el operador los ofrece como una alternativa al cliente para que realice llamadas de voz entre otras sucursales o algunos puntos de interés que también estén con el operador, este tipo de llamadas el cliente únicamente paga por un valor mensual o anual.

En cambio, una llamada que termina a otro operador y usa la red telefónica pública conmutada o PSTN por sus siglas en inglés (*public switched telephone network*) tiene un costo cobrado por minutos.

El operador para ambos servicios convierte la llamada de voz tradicional a digital y la envía por su red IP, como se explicó para convertirla en VoIP, por medio de codificadores que operan con el códec G.711 (64Kbps). Y se envía a su central de telefonía desde donde se distribuye a la red local o bien a la PSTN.

El operador posee un servidor que se encarga de conmutar las llamadas VoIP ya sean internas o bien que sean terminadas en la PSTN. Además, dicho

servidor se encarga de la tarificación, control y detalle de los minutos consumidos para cuando la llamada termina en la PSTN.

4.2.2. Topología de la red del operador

Como se mencionó, la red del operador tiene una topología en anillo, compuesta con cinco nodos y un nodo central, los cuales tienen funciones de nodos de segregación; además, están los nodos de distribución que son conectados a los nodos de segregación, de los nodos de distribución son conectados los ramales por donde son entregados los servicios a los clientes.

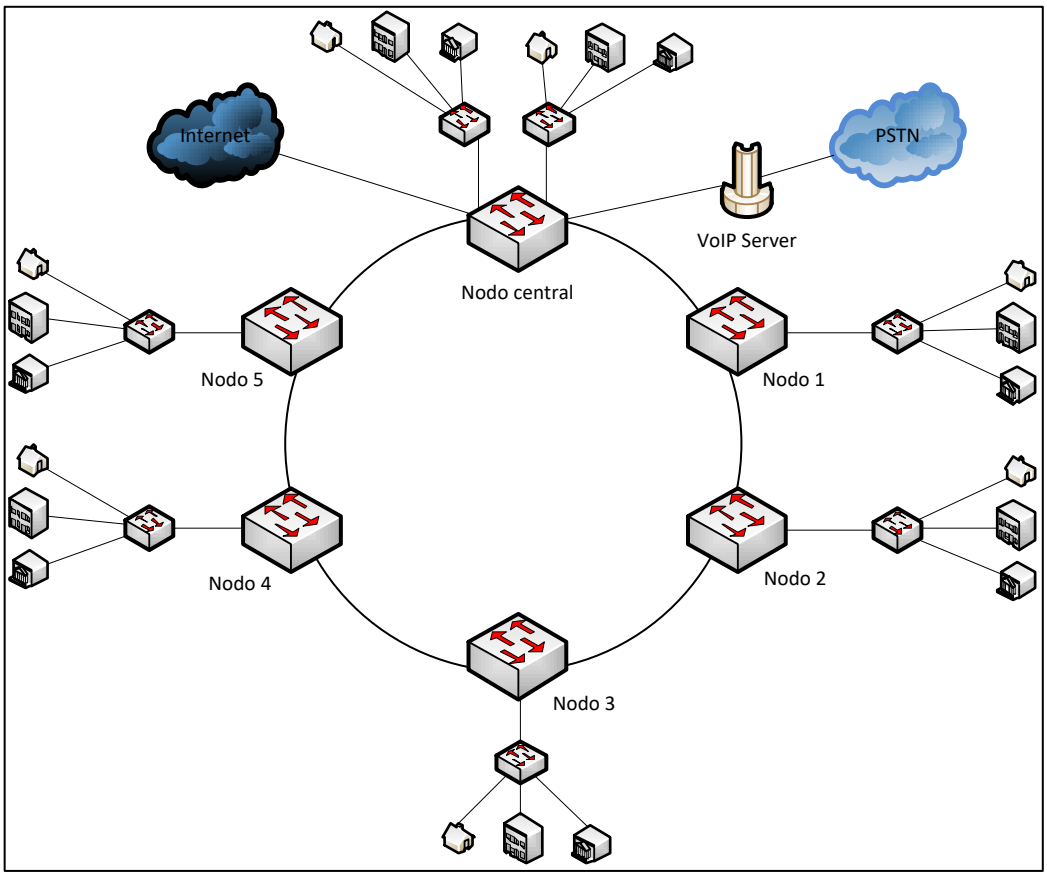
Actualmente, los *switchs* de distribución y de segregación cuentan con una densidad de 24 puertos, pero en el caso de los nodos de segregación cuentan con un módulo que puede ser intercambiable por interfaces de 1 *Gigabit* por segundo.

Los *switchs* de segregación actualmente utilizan un método de agregación entre sus interfaces para aumentar la capacidad del anillo principal; es decir, los *switchs* de segregación actualmente utilizan interfaces de 1 *gigabit* por segundo, pero han agregado 3 interfaces para alcanzar una capacidad de 3 *gigabit* por segundo en total.

Aunque el operador ha aprobado el emplear este método de agregación ha requerido que el mismo no sea empleado a más de 5 interfaces, es decir, que si este método es considerado como parte de las propuestas de solución la capacidad máxima que se puede alcanzar es la equivalente a 5 interfaces en agregación.

La topología actual del operador es mostrada en la figura 11.

Figura 11. **Topología de red propuesta**



Fuente: elaboración propia.

En la tabla XVI se muestra el inventario de la cantidad de enlaces o servicios que la red que el operador posee, y la distribución de los servicios y de los nodos en los que se encuentra conectado.

Tabla XVI. **Inventario de servicios sobre la red del operador**

	Total servicios datos + VoIP	Total servicios datos	Datos 1Mbps	Datos 3Mbps	Datos 5Mbps	Servicios VoIP
Nodo central	63	45	16	12	17	18
Nodo 1	39	24	12	9	3	15
Nodo 2	30	21	14	6	1	9
Nodo 3	45	34	17	4	13	11
Nodo 4	32	26	12	9	5	6
Nodo 5	13	9	4	3	2	4
Total	222	159	75	43	41	63

Fuente: elaboración propia.

Además, actualmente el operador ya reporta 438 310 minutos por año de llamadas que son terminadas a la PSTN.

El operador ha logrado estimar el crecimiento para cada servicio en particular de datos como servicios de voz y la cantidad minutos en llamadas. Ambos, basados en el comportamiento de otros años y el acercamiento que ha tenido con los clientes, sus proyecciones de crecimiento y la de otros clientes potenciales. En la tabla XVII se muestra la proyección para los próximos cinco períodos.

Tabla XVII. **Proyección de crecimiento del operador para 5 períodos**

Proyecciones del operador	0	1	2	3	4	5
% de crecimiento anual en Servicio Datos		9,1 %	9,3 %	9,5 %	9,4 %	9,5 %
Proyección crecimiento Servicio Datos 1Mbps	75	82	90	99	109	120
Proyección crecimiento Servicio Datos 3Mbps	43	47	52	57	63	69
Proyección crecimiento Servicio Datos 5Mbps	41	45	50	55	61	67
% de crecimiento anual en Servicio VoIP		10,1 %	11,3 %	12,4 %	13,1 %	14,0 %
Proyección crecimiento Servicio VoIP	63	70	78	88	100	114
% de crecimiento anual de minutos en Servicio VoIP		9,8 %	11,0 %	12,5 %	13,4 %	14,1 %
Proyección crecimiento minutos de telefonía a PSTN	438 310	481 265	534 205	600 981	681 513	777 607

Fuente: elaboración propia.

4.3. Análisis de la factibilidad técnica para la migración de la red del operador en STP a EAPS

La red del operador como se explicó actualmente opera con el protocolo STP, lo que significa que dicho protocolo provee el respaldo ante una falla para los servicios, empleando los procesos detallados en el capítulo 2; además, la red está configurada en capa dos por lo que cada uno de los servicios se separa de los demás empleando VLAN.

4.3.1. Problemática de la red del operador en STP

Actualmente, con STP ante una falla en una de las rutas del anillo, el tiempo que le toma al protocolo actuar y elegir un camino alterno para el envío de la información son casi 50 segundos en el peor de los casos, lo que no representa un problema para los servicios de datos, que representan el 71,6 % del total de los servicios brindados por el operador; con frecuencia la comunicación se restablece sin que los clientes realicen maniobras en sus equipos al punto que suele ser imperceptible para el usuario final.

Pero el operador ha visto que la demanda para transmitir servicios de voz ha ido en aumento; según las expectativas, en los próximos años podría acelerar su crecimiento; el operador conoce que este tipo de servicios ante una falla se verán afectados con interrupciones de la comunicación, mala calidad o degradación del servicio, y consecuentemente en una mala imagen de la empresa.

La causa principal para la interrupción en los circuitos son los cortes de fibra instalada a lo largo de la ciudad. El tendido de fibra es en gran parte del

anillo instalada de forma aérea, lo que incrementa la probabilidad de fallas en el anillo. Por lo general estas suceden de dos a tres veces por mes.

El operador considera necesario analizar las opciones con las que pueda reducir el tiempo de convergencia y el impacto en la calidad de los servicios, especialmente de los de voz, cuando una falla aparezca en la red.

4.3.2. Visión de la nueva red metro-Ethernet empleando EAPS

Para evaluar una solución a la problemática del operador, se presentan las siguientes alternativas:

- Opción 1: RSTP

La primera opción consiste en realizar un cambio en el protocolo empleado para la convergencia de la red y evitar que se creen *loops* por RSTP empleando *port fast* para reducir el tiempo de convergencia entre 400 a 600 milisegundos, empleando los mismos equipos *switches*.

- Opción 2: EAPS

La segunda opción consiste en sustituir los *switches* del anillo por otros que soporten el protocolo EAPS para manejar la convergencia y evitar *loops*.

- Opción 3: STP

La última opción consiste en no realizar ningún cambio a la red actual y continuar brindando los servicios de datos y de voz con el protocolo STP.

Para entender mejor las ventajas y desventajas de cada uno de estas opciones se provee en la tabla XVIII un comparativo para su análisis a nivel del protocolo que se encargará para la redundancia del anillo:

Tabla XVIII. **Comparativa de opciones para el operador por tipo de protocolo a utilizar**

	Opción 1: RSTP	Opción 2: EAPS	Opción 3: STP
Tiempo de convergencia (milisegundos)	400 a 600	50	50 000
Calidad de experiencia en voz (ante una falla) - según escala MOS/R	En el limite entre aceptable y no aceptable	Aceptable / deseable	Completamente no aceptable
Soportado SW de la red actual	Sí	No	Sí
Impacto por cambios necesarios	Medio	Alto	Ninguno

Fuente: elaboración propia.

Al observar esta comparativa de la tabla XVIII se identifica que la problemática del operador no es resuelta con la opción 3, ya que el tiempo de convergencia es mucho mayor al tiempo mínimo para no impactar en la calidad del servicio, según el requerimiento del operador.

Además, como se ha expuesto anteriormente, el operador ha visualizado la necesidad de aumentar la capacidad sobre su red con base en el crecimiento proyectado y considerando la capacidad de su red actual; será explicado en la sección 4.3.3 Análisis de costos, beneficios e inversión para ampliación de capacidad en *switches*; por lo cual, la opción 3 será descartada a partir de este momento y este estudio será enfocado únicamente basado en las otras dos opciones.

Recuérdese que el operador está buscando alternativas que puedan reducir el tiempo de convergencia para reducir el impacto en la calidad de los servicios al momento de suceder una falla y una conmutación de rutas, por lo que las opciones 1 y 2 son las opciones que son viables para su implementación y que ofrecen solución al requerimiento del operador.

La opción 2 es la que ofrece mejores beneficios en lo que respecta a la problemática del operador; brinda una reducción considerable al tiempo de convergencia ante una falla y, por consiguiente, en la calidad de experiencia de los usuarios al hacer uso de servicios de voz; pero esta opción 2 es la que requiere mayores cambios en la red.

En el caso de la opción 1, es completamente soportada por los equipos actualmente instalados en la red; no requiere mayores cambios en la red, aunque el tiempo de convergencia al andar entre los 400 a 600 milisegundos se encuentra en el límite, o inclusive superarlo, para mantener una calidad de experiencia aceptable.

4.3.3. Análisis de costos, beneficios e inversión para ampliación de capacidad en *switches*

En adelante del estudio solo se considerarán dos escenarios, ya que como se ha explicado el escenario de no realizar ningún cambio (opción 3) no es viable ya que el operador requiere realizar una ampliación en la capacidad de la red. El primero, de los dos escenarios ha estudiar, será con la opción de *switches* que soportan el protocolo RSTP; el segundo escenario será con la opción de *switches* que soportan el protocolo EAPS.

Con la topología actual de 6 nodos principales o de agregación y 7 nodos de acceso o distribución, se obtiene una suma total de 312 puertos, ya que todos los nodos son de 24 puertos. Para el período 5 de nuestro análisis se necesitarán 370 puertos, entre todos los servicios de datos y de VoIP; es necesario considerar *switches* de 48 puertos para los nodos de distribución, así se alcanzará una densidad máxima de 480 puertos. Además, actualmente ya se utiliza agregación de interfaces de 1 *gigabit* por segundo, se recomienda que los nuevos *switches* posean interfaces de 10 *gigabit* por segundo para los enlaces que componen el anillo.

Tomando en cuenta estas consideraciones de dimensionamiento, el escenario con protocolo RSTP será cubierto con equipos de la marca Cisco en la parte de agregación se implementarían los *switchs* WS-C3850-24F y para la parte de distribución el WS-C3850-48F. En el escenario con protocolo EAPS será Extreme, en la parte de agregación el modelo propuesto es X460-G2-24x-10GE4 y para la parte de distribución X460-G2-48x-10GE4.

Aunque varían en precio, ambas opciones tienen características muy similares en muchos aspectos incluyendo la densidad de puertos. Ambas opciones poseen interfaces de 10 *gigabit* por segundo. Aunque la opción de EAPS puede manejar más de un par de interfaces de 10 gigabit por segundo, a diferencia de la opción en RSTP que únicamente posee un módulo en 1 *gigabit* por segundo.

Ambas opciones pueden emplear el método de agregación para ampliar capacidad en el ancho de banda, y recordamos que el operador requirió que de usarse esta opción no debe ser superior a 5 interfaces agregadas.

En la tabla XIX se compara la utilización de capacidad de ancho de banda, en dimensionales de megabit por segundo, y su proyección de crecimiento con base en la proyección de ventas, la capacidad máxima de los *switches* considerando la capacidad actual y los dos escenarios, la opción con RSTP y la opción con EAPS.

Tabla XIX. **Comparativa ancho de banda en *switches***

	Períodos					
Comparativa ancho banda en switches	**0**	**1**	**2**	**3**	**4**	**5**
Capacidad ancho banda SW actuales [Mbps]	3 000	3 000	3 000	3 000	3 000	3 000
Capacidad ancho banda SW futuros con RSTP [Mbps]		10 000	10 000	10 000	10 000	10 000
Capacidad ancho banda SW futuros con EAPS [Mbps]		10 000	10 000	10 000	10 000	20 000
Utilización Ancho Banda Proyectado [Mbps]	2 480	2 852	3 536	4 845	7 025	10 397

Fuente: elaboración propia.

En la tabla XII, debido a la limitante de los *switches* con la opción de RSTP de solo una interface de 10 *gigabit* por segundo, para el período 5 la capacidad máxima es superada. Mientras que para el escenario con la opción en EAPS, ya que posee más de un par de interfaces de 10 *gigabit* por segundo puede considerar un par de puertos en agregación para cubrir esta demanda.

En la tabla XX se compara la densidad de puertos ocupados en la red actual, la proyección de crecimiento con base en la proyección de ventas, y la densidad de puertos con la opción en RSTP y la densidad de puertos con la opción en EAPS.

Tabla XX. **Comparativa densidad de puertos en *switches***

	Períodos					
Comparativa densidad de puertos en switches	**0**	**1**	**2**	**3**	**4**	**5**
Densidad puertos SW actuales [puertos]	312	312	312	312	312	312
Densidad puertos SW Futuros con RSTP [puertos]		480	480	480	480	480
Densidad puertos SW Futuros con EAPS [puertos]		480	480	480	480	480
Utilización puertos proyectado [puertos]	222	244	270	299	333	370

Fuente: elaboración propia.

En la tabla XX, se detalla la densidad de puertos de ambos escenarios que cubren satisfactoriamente la demanda de puertos en el período evaluado.

En la tabla XXI se muestra el resumen de la comparativa de costos de ambas opciones.

Tabla XXI. **Comparativa de costos para ampliación de *switches***

	Cambios a *switchs* con RSTP	**Cambios a *switchs* con EAPS**
Costos cambio de *switchs* para ampliación de capacidad	**Opción 1**	**Opción 2**
Switchs nuevos	$ 42 000,00	$ 42 000,00
Partes de reemplazo *switchs* nuevos	$ 2 500,00	$ 6 600,00
Tarjetas de interconexión	$ 7 400,00	$ 7 400,00
Software y licencias RSTP	$ 1 200,00	$ -
Software y licencias EAPS	$ -	$ 8 000,00
Servicios de instalación y configuración de equipos nuevos	$ 12 000,00	$ 12 000,00
Capacitación técnica para operación switches nuevos	$ 1 200,00	$ 10 000,00
Migración de servicios	$ 3 500,00	$ 3 500,00
Servicios de pruebas y confirmación	$ 3 500,00	$ 3 500,00
Otros gastos de instalación	$ 5 000,00	$ 5 000,00
Recurso humano	$ 7 800,00	$ 7 800,00
Total de costos	$ 86 100,00	$ 105 800,00

Fuente: elaboración propia.

Además, como se mencionó, el operador considera que puede tener algún beneficio por la reutilización de los equipos y venta de algunas otras partes. Ya que la opción 1, contempla el continuar usando en la red *switches* del fabricante actual, se estima que la oportunidad de reutilización es mayor con respecto a la opción 2. En cambio, la cantidad de partes que pueden ser vendidas es mayor en la opción 2. Ver en la tabla XXII el resumen de los posibles beneficios en ambas opciones.

Tabla XXII. **Comparativa de beneficios para ampliación de *switches***

Beneficios cambio de *switchs* para ampliación de capacidad	Opción 1	Opción 2
Ahorro por reutilizar *switchs* para red	$ 13 000,00	$ 4 800,00
Ahorro por reutilizar *switchs* para partes de reemplazo	$ 3 200,00	$ 800,00
Venta de equipos sin reutilizar	$ 1 200,00	$ 6 600,00
Total de beneficios	$ 17 400,00	$ 12 200,00

Fuente: elaboración propia.

Por lo tanto, con base en las tablas XXI y XXII, se puede obtener la comparativa de la inversión total necesaria para ambas opciones, ver tabla XVI.

Tabla XXIII. **Comparativa de inversión total para ampliación de *switches***

Inversión cambio de *switchs*	Opción 1	Opción 2
Inversión Inicial	$ 68 700,00	$ 93 600,00

Fuente: elaboración propia.

Aunque la inversión de la opción 2 es mayor en $24 900, el operador considera que la inversión de esta tecnología y la mejora en tiempos de respuesta podrá obtener beneficios adicionales en rubros como:

- Ahorro en llamadas en centro de soporte
- Ahorro en imagen por reducción en tiempo de falla
- Diversificación de servicios y productos
- Ampliación en volumen de operación y crecimiento

Los detalles de estos beneficios serán incluidos en la matriz financiera para el análisis de la factibilidad económica.

4.3.4. Pasos para la transición a la nueva red

Para entender mejor la factibilidad de la opción con RSTP y de la opción con EAPS, a continuación, los pasos generales para alcanzar la migración de la red actual del operador con STP a la red operando con RSTP o EAPS.

4.3.4.1. Migración de STP a RSTP

La migración a RSTP, es decir la opción 1, consiste básicamente en dos pasos que deberán ser programados en actividades de bajo tráfico, para reducir el impacto en los servicios sobre la red:

- Actualizar el sistema operativo de cada uno de los nodos para que sea soportado RSTP como parte de sus configuraciones.

- Realizar el proceso de migración por nodo de las configuraciones en RSTP, aprovechando que RSTP es compatible con STP y aunque los demás nodos aún no operen en RSTP y solo en STP pueden coexistir, aunque no se tendrán todos los beneficios de RSTP hasta que todos los nodos sean migrados.

Cuando haya finalizado la configuración de RSTP en todos los nodos, se podrá dejar únicamente operando este protocolo con lo que se obtendría el resultado deseado.

4.3.4.2. Migración de STP a EAPS

Como se mencionó, la migración de la red actual a la red empleando EAPS será la migración con mayor impacto. La propuesta al operador consiste en dos pasos:

- Adquirir el equipo necesario que soporte dicho protocolo, que además maneje STP, para realizar la migración de los equipos actuales por los nuevos conteniendo las configuraciones de la red en STP y además en EAPS.

- Luego de completar la migración de los seis nodos, planear la actividad para migrar todos los servicios al anillo EAPS. Con seguridad el diseño y ejecución de la migración representarán más horas de trabajo con respecto a la opción de migración a RSTP.

4.4. Análisis económico de la migración a EAPS

En este punto y con la información se realizará un análisis económico de la migración a EAPS para evaluar la rentabilidad de dicha migración, para lograrlo se utilizarán herramientas y la interpretación de sus resultados: valor presente neto (VPN) y la tasa interna de retorno (TIR).

Para realizar el análisis económico se utilizará la matriz financiera que incluyen gastos e ingresos, por la cual se encontrarán los datos del valor

presente neto (VPN) y de la tasa interna de retorno (TIR). En el análisis consideraremos una tasa de ganancia de 7 % no acumulativa, que es el porcentaje típico de pago anual por bancos locales o tasa interna aceptable.

Los criterios que se proponen para el proyecto sea considerado con factibilidad económico se describen a continuación:

- El valor presente neto (VPN) deberá ser mayor o igual a cero
- La tasa interna de retorno (TIR) sea mayor que la tasa interna aceptable
- La relación de beneficio/costo sea igual o mayor a cero

Considerando las proyecciones de crecimiento de la tabla XVII, y los precios unitarios de los servicios que ofrece el operador descritos en la tabla XVII a continuación. Se podrá obtener la matriz financiera y el flujo de efectivo proyectado a 5 períodos para el análisis respectivo de los criterios de factibilidad económica.

Tabla XXIV. **Precios unitarios de los servicios del operador**

Precios unitarios	
Precio unitario servicio datos 1Mbps	$ 95,00
Precio unitario servicio datos 3Mbps	$ 210,00
Precio unitario servicio datos 5Mbps	$ 325,00
Precio unitario servicio VoIP	$ 245,00
Precio de minuto de telefonía a PSTN	$ 0,20

Fuente: elaboración propia.

Por un lado, en la tabla XXV se muestran los costos como parte de la matriz financiera.

Tabla XXV. **Matriz financiera – costos**

	Períodos					
Costos	**0**	**1**	**2**	**3**	**4**	**5**
Switches nuevos	$ 42 000,00	$ -	$ -	$ -	$ -	$ -
Partes de reemplazo switches nuevos	$ 6 600,00	$ -	$ -	$ -	$ -	$ -
Tarjetas de interconexión	$ 7 400,00	$ -	$ -	$ -	$ -	$ -
Software y licencias para EAPS	$ 8 000,00	$ -	$ -	$ -	$ -	$ -
Servicios de instalación y configuración de equipos nuevos	$ 12 000,00	$ -	$ -	$ 1 200,00	$ -	$ -
Capacitación técnica para operación switches nuevos	$ 10 000,00	$ -	$ -	$ -	$ -	$ -
Migración de servicios	$ 3 500,00	$ -	$ -	$ -	$ -	$ -
Servicios de pruebas y confirmación	$ 3 500,00	$ -	$ -	$ 450,00	$ -	$ -
Otros gastos de instalación	$ 5 000,00	$ -	$ -	$ 175,00	$ -	$ -
Mantenimiento de equipos	$ -	$ 2 300,00	$ 2 300,00	$ 2 400,00	$ 2 400,00	$ 2 400,00
Reparación de equipos	$ -	$ 1 200,00	$ 1 200,00	$ 1 245,00	$ 1 245,00	$ 1 245,00
Costos de comunicación	$ -	$ 250 000,00	$ 250 000,00	$ 265 000,00	$ 265 000,00	$ 265 000,00
Actualización de software	$ -	$ 850,00	$ 850,00	$ 925,00	$ 925,00	$ 925,00
Soporte anual para el fabricante	$ -	$ 1 300,00	$ 1 300,00	$ 1 350,00	$ 1 350,00	$ 1 350,00
Instalación de circuitos de expansión	$ -	$ -	$ -	$ 2 300,00	$ -	$ -
Expansión en switches nuevos	$ -	$ -	$ -	$ 450,00	$ -	$ -
Tarjetas de interconexión por expansión	$ -	$ -	$ -	$ 1 300,00	$ -	$ -
Recurso humano	$ 7 800,00	$ 7 800,00	$ 7 800,00	$ 7 800,00	$ 7 800,00	$ 7 800,00
Total de costos	$ 105 800,00	$ 263 450,00	$ 263 450,00	$ 284 595,00	$ 278 720,00	$ 278 720,00

Fuente: elaboración propia.

En la tabla XIX se detallan los beneficios como parte de la matriz financiera.

Tabla XXVI. **Matriz financiera – beneficios**

	Períodos					
Beneficios	**0**	**1**	**2**	**3**	**4**	**5**
Ahorro por reutilizar switches para red	$ 4 800,00	$ -	$ -	$ -	$ -	$ -
Ahorro por reutilizar switches para partes de reemplazo	$ 800,00	$ -	$ -	$ -	$ -	$ -
Venta de equipos sin reutilizar	$ 6 600,00	$ -	$ -	$ -	$ -	$ -
Ahorro en llamadas en centro de soporte	$ -	$ 3 500,00	$ 3 750,00	$ 4 300,00	$ 4 675,00	$ 5 100,00
Ahorro en imagen por reducción en tiempo de falla	$ -	$ 12 000,00	$ 13 100,00	$ 14 650,00	$ 16 240,00	$ 18 090,00
Ahorro en costos de operación y mantenimiento	$ -	$ 7 000,00	$ 7 000,00	$ 7 000,00	$ 7 000,00	$ 7 000,00
Mejor y facilidad en administración de la red	$ -	$ 2 300,00	$ 2 300,00	$ 2 300,00	$ 2 300,00	$ 2 300,00
Diversificación de servicios y productos	$ -	$ 21 000,00	$ 18 000,00	$ 19 000,00	$ 17 500,00	$ 17 500,00
Incursión en nuevos mercados	$ -	$ 31 000,00	$ 30 000,00	$ 32 500,00	$ 30 000,00	$ 29 800,00
Ampliación en volumen de operación y crecimiento	$ -	$ 39 000,00	$ 47 000,00	$ 54 000,00	$ 61 000,00	$ 75 000,00
Proyección de ventas datos	$ -	$ 32 285,00	$ 35 720,00	$ 39 250,00	$ 43 410,00	$ 47 665,00
Proyección de ventas VoIP	$ -	$ 17 150,00	$ 19 110,00	$ 21 560,00	$ 24 500,00	$ 27 930,00
Proyección de ventas minutos VoIP	$ -	$ 96 253,00	$ 106 841,00	$ 108 176,58	$ 122 672,34	$ 139 969,26
Total de beneficios	$ 12 200,00	$ 261 488,00	$ 282 821,00	$ 302 736,58	$ 329 297,34	$ 370 354,26

Fuente: elaboración propia.

En la tabla XXVII, por último, se resume el flujo neto efectivo de matriz financiera.

Tabla XXVII. **Matriz financiera – flujo neto efectivo**

	Períodos					
Flujo neto efectivo	**0**	**1**	**2**	**3**	**4**	**5**
Flujo neto efectivo (beneficios - costos)	$ -93 600,00	$ -1 962,00	$ 19 371,00	$ 18 141,58	$ 50 577,34	$ 91 634,26

Fuente: elaboración propia.

4.4.1. Valor presente neto (VPN)

Conn base en la matriz financiera se obtienen los siguientes datos para calcular el valor presente neto.

Tabla XXVIII. **Valor presento neto (VPN)**

Valor presente neto considerando 7 % de interés	
Año 0	$ -93 600,00
Año 1	$ -1 962,00
Año 2	$ 19 371,00
Año 3	$ 18 141,58
Año 4	$ 50 577,34
Año 5	$ 91 634,26

VPN	$ 37 583,03

Fuente: elaboración propia.

4.4.2. Tasa interna de retorno (TIR)

Con base en la matriz financiera se obtienen los siguientes datos para calcular la tasa interna de retorno.

Tabla XXIX. **Tasa interna de retorno (TIR)**

Tasa interna de retorno considerando 7 % de interés anual	
Año 0	$ -93 600,00
Año 1	$ -1 962,00
Año 2	$ 19 371,00
Año 3	$ 18 141,58
Año 4	$ 50 577,34
Año 5	$ 91 634,26
TIR	17 %

Fuente: elaboración propia.

4.4.3. Análisis beneficio/costo

Con base en la matriz financiera se obtienen los siguientes datos para realizar el análisis beneficio/costo.

Tabla XXX. **Análisis beneficio / costo**

Valor presente neto considerando 7 % de interés anual		
Períodos	**Beneficios**	**Costos**
Año 0	$ 12 200,00	$ 105 800,00
Año 1	$ 261 488,00	$ 263 450,00
Año 2	$ 282 821,00	$ 263 450,00
Año 3	$ 302 736,58	$ 284 595,00
Año 4	$ 329 297,34	$ 278 720,00
Año 5	$ 370 354,26	$ 278 720,00
VPN	$ 1 183 185,22	$ 1 145 602,19
Beneficio / costo	1,03	

Fuente: elaboración propia.

En resumen y considerando los criterios de aceptación:

- El valor presente neto (VPN) $ 37 583,03, es mayor que cero.
- La tasa interna de retorno (TIR) 17 % es mayor que la tasa interna estimada del 7 %.
- La relación de beneficio/costo 1,03 es mayor que uno.

Por lo que, existe la factibilidad técnica para la migración de los servicios a una red tipo anillo basada en el protocolo EAPS; también, existe factibilidad económica considerando las proyecciones que el operador ha presentado, y por los beneficios mencionados en la sección 4.3.3, por considerar la opción de ampliar la capacidad de los equipos empleando tecnología que soporte el protocolo EAPS. Dentro de los beneficios descritos se encuentran: diversificación de servicios y productos y ampliación en volumen de operación y crecimiento.

CONCLUSIONES

1. Topologías en anillo requieren un protocolo de red para cumplir con tres funciones importantes:

   - Evitar *loops*
   - Selección de caminos alternos
   - Selección ruta única

2. EAPS ejecuta la conmutación en 50 milisegundos, que es menor al tiempo que les toma los protocolos STP y RSTP.

3. RSTP posee un tiempo de conmutación de 400 a 600 milisegundos por lo que el uso de este protocolo está en el límite permitido para no tener impacto en servicios VoIP.

4. La migración de STP a EAPS, en la red propuesta para el estudio, es factible técnicamente bajo los procedimientos descritos.

5. La migración de STP a EAPS, en la red propuesta para el estudio, es factible económicamente bajo las condiciones descritas para el estudio.

RECOMENDACIONES

1. En redes metro-Ethernet siempre que se decida una actualización de equipo o de software para soportar la aplicación de protocolo EAPS se debe considerar el impacto significativo en que pueden verse involucrado los servicios que brinda el operador.

2. El proceso de migración de STP a RSTP o EAPS debe considerarse de un modo progresivo y controlado para asegurar el mínimo impacto durante dicho proceso para los servicios que brinda el operador.

3. Considerar como parte del proceso de migración pruebas de configuración de parámetros propios del nuevo protocolo y definir indicadores de desempeño claves que puedan ser monitoreados durante y posterior al proceso de migración.

4. El operador ha proporcionado como parte del estudio una proyección agresiva en crecimiento de servicios, por lo que debe garantizar dicha ejecución para no poner en riesgo la rentabilidad de la implementación de esta solución.

BIBLIOGRAFÍA

1. International Telecommunications Union. *E-model Tutorial.* [En línea]. <https://www.itu.int/ITU-T/studygroups/com12/emodelv1/tut.htm>. [Consulta: 26 de marzo de 2011].

2. Lambert M. Tennoe, Mariam T. Henssonow, Susan F. Surhone. *Ethernet Automatic Protection Switching.* Chicago: Betascript Publishing, 2010. 514 p.

3. S. Shah, M. Yip. *Request for comments: 3619 R*. EE.UU.: Atkinson Extreme Networks, 2003. 1202 p.

4. Todd Lammle CCSI. *Cisco Certified Network Associate.* 6a ed. London: Wiley Publishing, Inc., 2008. 815 p.

APÉNDICE

Apéndice 1. Valores provisionales de planificación para el factor de degradación de equipo, Ie

Este anexo proporciona información y fue tomada del *Apendice I de la ITU-T Recomendación G.113*-200102 sobre los valores disponibles del factor de degradación de equipo, Ie. El cuadro de la tabla XII expone los valores Ie y se refiere a condiciones no procedentes de error. Para borrados de trama y errores debidos a la propagación o pérdida de paquete, no se dispone de valores definitivos que sean válidos para más de un códec o familia de códec. Se dan ejemplos de valores de Ie en condiciones de pérdida de paquetes.

.

Valores provisionales de planificación para el factor de degradación del equipo Ie

Pérdida de paquetes (%)	G.729-A + VAD	G.723.1-A + VAD 6,3 kbit/s	GSM EFR
0	11	15	5
0,5	13	17	(Nota 2)
1	15	19	16
1,5	17	22	(Nota 2)
2	19	24	21
3	23	27	26
4	26	32	(Nota 2)
5	(Nota 2)	(Nota 2)	33
8	36	41	(Nota 2)
16	49	55	(Nota 2)

Fuente: elaboración propia.