UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

IMPLEMENTACIÓN DE UNA RED DE DATOS POR PUERTO EXTENDIDO

T E S I S

PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A:

MIGUEL GONZÁLEZ POMPOSO

DIRECTOR DE TESIS:
ING. JOSÉ ALBERTO ÁVALOS VÉLEZ

Ciudad Universitaria, Agosto de 2013

Agradecimientos

A mis padres Justina Pomposo y Juan González que me han brindado su amor, paciencia y gran apoyo a lo largo de mi vida, tanto en mi formación como persona y en la profesional, sus consejos y enseñanzas han sido fundamentales para poder llegar a estas instancias.

A mis hermanas Gaby y Laura por la confianza y el apoyo que me han brindado durante todos los años que hemos compartido y aprendido juntos.

A mis profesores, que desde el comienzo de esta gran historia me han compartido de sus conocimientos y experiencias que me serán de gran ayuda para afrontar los problemas de hoy y del mañana.

A la Universidad Nacional Autónoma de México y a la Facultad de Ingeniería por ofrecerme el lugar perfecto para estudiar y desarrollarme profesionalmente y culturalmente, y porque me ha permitido conocer a personas que me han ofrecido su valiosa amistad y sus conocimientos, mismos que he tomado parte de mi formación y les seré muy agradecido.

A José Alberto, mi director de tesis por haber confiado en mí, por el apoyo y conocimientos que ha compartido conmigo para hacer este trabajo saliera adelante.

Índice general

Índice de figuras

Introducción

Actualmente la administración de una red de datos es tan compleja o sencilla debido a su diseño y tamaño. Es evidente que al crecer el tamaño de la red, el nivel de la administración y mantenimiento requiere un mayor trabajo y atención de los problemas. De esta manera se hace imprescindible contar con un diseño de la red física y lógica adecuada para que se logre llevar a cabo la gestión de la red, la detección de errores, la detección de fallas y una pronta solución de los mismos. Esa infraestructura, además de permitir lo mencionado, también debe proveer seguridad en la transmisión de la información, así como lograr una comunicación eficiente.

En el Instituto de Educación Media Superior del Distrito Federal (IEMS) no existía un esquema de red de datos, pues constaba originalmente de la red local para cada uno de los planteles, cada una conectada a Internet a través de la línea de ADSL que permitía la comunicación hacia Internet, tal como están conectada una red local de un hogar. Si existía la necesidad de compartir información entre planteles, el uso de Internet se hacía inminente. Esto era ineficiente, inadecuado que impedía el aprovechamiento máximo de los recursos de cada plantel para la Institución general. Los riesgos de la pérdida de la disponibilidad es latente en una Institución con una red con ese funcionamiento y estructura de la red, cada nodo de datos es propenso a que la información que se transmite pierda integridad y autenticidad ya que los datos circulan a través de Internet y no por medio de una red privada que represente a la institución.

Debido a lo comentado anteriormente se propone este proyecto para el diseño de una red que integre a todos los planteles de la Institución que se encuentran aislados uno del otro. Se busca que sea una red escalable, que implemente seguridad en la transmisión de los datos, que sea administrable y que económicamente represente beneficios. Esta red de datos plantea un modelo de infraestructura de red que permite que las redes locales de cada plantel sean parte de una red de datos única, la información que se comparte a nivel interinstitucional es privada, esos datos que pueden sensibles o sólo informativos circulan a través de la red de la Institución y no por medio de Internet. Correo electrónico y fax institucional, la transferencia de archivos, compartición de recursos en red como impresoras, uso de bases de datos y servidores compartidos es local, además de que se tiene un control de los datos que salen hacia Internet.

La red de datos que se plantea se conectará a través de puertos extendidos, es decir, las veinte redes locales de los planteles que se encuentran distantes geográficamente una de la otra se comunicarán entre sí de una manera directa, esto gracias la conexión que se establecerá con un dispositivo central que unificará la comunicación. El uso de estos enlaces proporciona seguridad a la red ya que se establecerá un camino privado entre los planteles y estos podrán compartir información entre sí sin la necesidad de salir a Internet.

Además, debido a que la red estará compuesta por dispositivos capaces de soportar la carga de trabajo para cada uno de los planteles, se necesitan dispositivos que garanticen eficiencia y funcionalidad además de representar un impacto económico bajo. La implementaciones se basarán en sistemas operativos libres con características que ofrecen gran funcionalidad, tal es el caso del uso de pfSense como primera instancia, y como una propuesta de mejora se plantea la instalación y puesta en operación de dispositivos especializados en los que se aproveche la implementación de un protocolo de enrutamiento dinámico para proporcionarle a la red rápida convergencia.

Con la introducción de equipos de red comerciales, la implementación de un protocolo de ruteo dinámico en la Red Institucional del IEMS permitirá una rápida convergencia de la misma y que estará compuesta de una topología centralizada y jerarquizada, misma a la que se aplicarán políticas de seguridad a nivel hardware y de usuarios finales.

Debido a que la red propuesta estará basada principalmente en la implementación de conexiones por medio de puertos extendidos, se contará con los Routers de acceso, Switches e infraestructura adecuada para poder ofrecer soporte técnico remoto que atienda problemas que ocurran en horarios pico de trabajo principalmente. La necesidad de viajar hasta cada una de las redes de datos para resolver un problema por parte de los administradores de red que

se ubican en las oficinas centrales concluye con la implementación de esta red ya que cada dispositivo podrá ser monitorizado y alcanzable remotamente para su administración y resolución de incidencias.

Debido a las características de los puertos extendidos y a la seguridad que brindan, la implementación de dispositivos para ofrecer seguridad en la red se ubicará en un solo punto de la red y no en diversos puntos como se podría realizar. Un punto importante en la red son las salidas a Internet a toda la institución, y es en este lugar de la red en el que pasa todo el tráfico de las redes locales hacia Internet. OpenBSD será el sistema que se implementará en ese sitio de la red para que se encargue de la salida del tráfico, e implementación de la seguridad, además de que es un sistema muy robusto y el más seguro.

Asimismo, este documento tiene como propósito crear un modelo que sea utilizable en cualquier red de datos con la misma problemática y con los mismos requerimientos, ya que este trabajo no busca que sea únicamente una solución única a un problema en específico, sino se trata de un modelo que sea funcional para cualquier organización.

1

Conceptos generales

1.1 Redes de datos

En el siglo XVIII se dio la era de los sistemas mecánicos que produjo a su vez a las Revoluciones Industriales. En el siglo XIX se facilitó el auge de la máquina de vapor. Sin embargo, en el siglo XX, el desarrollo clave ha sido la tecnología para la recopilación, procesamiento y distribución de la información. Asimismo, se han dado numerosos desarrollos como las redes telefónicas, las redes de radio y televisión, el nacimiento y crecimiento sin precedente de la industria de la computación, la comunicación satelital y por supuesto, Internet.

Debido al avance vertiginoso de la tecnología, en el siglo XXI se está dando la convergencia de las áreas mencionadas. Hoy por hoy las organizaciones que cuentan con numerosas oficinas distribuidas geográficamente buscan revisar el estado de todas estas con sólo un click.

La industria de los equipos de cómputo es joven pero con un crecimiento sorprendente en un periodo de tiempo corto si se compara con otras como la automovilística por ejemplo. En las primeras dos décadas del desarrollo de la computación, instituciones medianas o universidades contaban con uno o dos dispositivos de cómputo que ocupaban un cuarto entero cada uno, y, mientras más grande la institución, se contaba con un mayor número de estos equipos.

Actualmente, el poder de procesamiento de los equipos de cómputo es mucho mayor que en los primeros años en los que se desarrollaron, y el tamaño de los mismos ha disminuido. Este impulso de los dispositivos junto con el de las comunicaciones ha cambiado la organización de los sistemas de cómputo. Uno de los conceptos dominantes de los "centros de cómputo" como un cuarto con una computadora gigante en el que los usuarios llevaban su trabajo para que se procesara hoy es totalmente obsoleto. El modelo viejo en el que una sola computadora sirve a toda una organización tiene que ser reemplazado por el esquema en el que un número grande de dispositivos interconectados hacen el trabajo y comparten información. Estos sistemas son llamados Redes de Datos.

1.1.1 Definición de una red de datos

En la actualidad el crecimiento de la tecnología ha sido vertiginoso y la comunicación entre individuos y organizaciones es un aspecto fundamental que se ha provocado con dicho desarrollo. Esto ha permitido que los usuarios se comuniquen desde cualquier lugar gracias a casi cualquier dispositivo, ya sea desde un teléfono celular hasta una computadora portátil. Además, cientos de miles de organizaciones se comunican entre sí y comparten recursos, sin importar su localización, y todo es gracias a las redes de datos.

Una red de datos se define como el conjunto de dispositivos que se interconectan entre sí gracias a medios físicos o inalámbricos y que son utilizados para la transmisión de mensajes y uso de servicios a través de la misma, siguiendo un conjunto de reglas y procesos que regulan la comunicación.

Hoy en día las redes de datos tienen un impacto importante en las actividades de diversas organizaciones y empresas en sus procesos de producción, organización del trabajo, compartición de recursos y de información principalmente, permitiéndoles la eficiencia y la minimización de costos. A usuarios comunes les permite el establecimiento de comunicación sin importar su ubicación geográfica y horario que desee, de manera privada o pública por medio de redes sociales. De esta manera se establece que las redes de datos deben cumplir con las siguientes características importantes sobre la información transmitida: *Confidencialidad, Integridad* y *Disponibilidad de la información.*

La comunicación a través de redes de datos se lleva a cabo gracias a los protocolos de comunicación. Un protocolo de comunicación es un conjunto de reglas que establecen el cómo se establecerá la comunicación entre los dispositivos. Se elegirá el protocolo adecuado dependiendo de los requerimientos de la red, tipo de aplicación que intenta la comunicación, medios de transmisión utilizados y confiabilidad de transmisión que se desea.

De la misma forma, los dispositivos y medios de transmisión trabajan bajo estándares que garantizan su interoperabilidad entre dispositivos de diferentes fabricantes. Los estándares son un grupo de normas que contienen especificaciones técnicas que deben seguir los fabricantes y empresas para que los dispositivos de red puedan trabajar entre sí.

Las redes de datos son muy importantes y tienen diversos usos, los más comunes son los siguientes:

- ***Aplicaciones de negocios***: Las compañías tienen un número substancial de computadoras, algunas de estas empresas tienen un dispositivo por cada empleado para la realización de una actividad determinada. El uso más importante que se le da a una red de datos en una empresa es compartir recursos, mismos que están disponibles para todos, como programas, equipamiento y datos principalmente. También los recursos físicos son compartidos, como impresoras y sistemas de recuperación.

  El acceso de los usuarios de la red a estos recursos puede ser de manera local o de manera remota, esta última a través de redes VPN para mantener la confidencialidad de los datos.

- ***Aplicaciones en el hogar***: Una de las razones principales por las que el auge de las computadoras personales se dio en sus inicios fue para el procesamiento de palabras y juegos. Recientemente, la más grande razón para la compra de computadoras fue probablemente el acceso a Internet. Ahora, muchos dispositivos electrónicos tales como *set-top boxes*, consolas de videojuegos, relojes, entre otros, cuentan con computadoras embebidas y tarjetas de red, especialmente inalámbricas que se conectan a las redes en los hogares y que son usadas ampliamente para el entretenimiento, incluyendo la escucha, la observación y creación de música, fotos y video, mejor conocido el conjunto de estos como multimedia.

  El acceso a Internet provee conectividad a los usuarios desde sus casas a computadoras remotas. Tal como las compañías, los usuarios caseros pueden tener acceso a información, comunicación con otras personas y comprar productos y servicios por medio del *e-commerce*.

- ***Usuarios móviles***: Computadoras móviles, tales como las laptops, tabletas y los dispositivos celulares (*smartphones*) son uno de los segmentos con más rápido crecimiento en la industria de la computación. La venta de estos dispositivos han superado a la de computadoras de escritorio. La preferencia de esta tecnología se ha dado porque las personas a menudo quieren usar sus dispositivos móviles para leer y enviar correos electrónicos, *tweets*, ver películas, descargar música, jugar juegos o simplemente navegar en la web por información. Quieren hacer todo lo que hacen en casa y en la oficina y, naturalmente desean hacerlo desde cualquier lugar, ya sea desde tierra, en el mar o en el aire.

  La conectividad a Internet habilita a muchos de estos usuarios. Desde la imposibilidad de tener conexión alámbrica en automóviles, barcos y aeroplanos, existe un interés grande en las redes inalámbricas. Redes celulares operadas por las compañías telefónicas son un tipo de redes inalámbricas que ofrecen cobertura a los teléfonos móviles. *Hotspots* inalámbricos basados en el estándar **IEEE 802.11** son otro tipo de redes inalámbricas para computadoras móviles. Estos dispositivos cubren cafés, hoteles, aeropuertos, escuelas, trenes y aviones. Cualquiera con un dispositivo portátil puede conectarse a Internet a través del *hotspot*, equipo que está conectado a su vez a una red alámbrica.

1.1.2 Clasificaciones de las redes de datos

Las redes de datos se pueden clasificar en varios tipos, ya sea por el alcance en metros o kilómetros que tiene la red, por la forma en que están conectados físicamente los dispositivos, o por la manera en que transmiten la información, es decir, la tecnología de la conexión.

A continuación se presentan esas clasificaciones y a su vez los tipos de redes según la clasificación en turno.

1.1.2.1 Clasificación por tecnología de transmisión

Hay algunos tipos de tecnología de transmisión que son usados ampliamente: enlaces broadcast, enlaces Punto a punto y enlaces Lan-to-Lan (puertos extendidos) que determinan cómo se comportará el envío de paquetes entre dispositivos.

Enlaces Punto a Punto

Estos conectan pares de máquinas individuales. Para ir de la fuente al destino en una red hecha por enlaces Punto a punto, los mensajes (paquetes) podrían cruzar por medio de uno o más dispositivos. La transmisión punto a punto con exactamente un transmisor y un receptor es llamado algunas veces *unicasting*.

Enlaces de este tipo pueden ser establecidos por interfaces de red que trabajen bajo el protocolo **SONET** (**Synchronous Optical NETwork**) y SDH (**Synchronous Digital Hierarchy**) que surgieron para estandarizar la comunicación punto a punto que realizaban los diferentes sistemas de **TDM** (**Time división Multiplexing**) de las compañías telefónicas en los inicios de la fibra óptica. El funcionamiento del protocolo PPP sobre SONET/SDH se puede encontrar detalladamente en el **RFC 1619.**

Enlaces de broadcast

En una red de *broadcast*, el canal de comunicación es compartido por todas las máquinas en una red. Los paquetes enviados por una máquina son recibidos por todos los demás dispositivos. Cada máquina que recibe el paquete revisa el campo de dirección de destino, si es recibido por la máquina destino, procesa el paquete; si el destinatario es para otra máquina, se ignora.

La tecnología que interconecta dispositivos por enlaces de broadcast es Ethernet, que se encuentra dividido en Ethernet clásico y Ethernet conmutado, en este último se utilizan switches que conectan diferentes computadoras. Las dos divisiones de Ethernet tienen pequeñas diferencias. Ethernet clásico es la forma original que funciona a tasas de velocidad de 3 a 10 Mbps, mientras que Ethernet conmutado va de 100 Mbps, 1000 Mbps y 10,000 Mbps, llamados fast Ethernet, gigabit Ethernet y 10 gigabit Ethernet. En práctica, únicamente Ethernet conmutado es usado hoy en día.

El estándar que trata el funcionamiento de Ethernet a profundidad es el **IEEE 802.3**.

Enlaces LAN-to-LAN como puerto extendido (L2L)

Un enlace L2L es un enlace dedicado que es provisto por el Proveedor de Servicios y es utilizado para conectar dos redes LAN separadas geográficamente. Un enlace LAN-to-LAN es construido físicamente con fibra óptica o cables de cobre en un tendido de cableado sobre una ciudad, junto con los cableados privados y públicos. Estos enlaces cuentan con dispositivos intermedios que utiliza el proveedor de servicios para proporcionar el transporte de los datos extremo a extremo. En cada una de las redes LAN del cliente se entrega una punta del enlace con un conector que, según la capacidad de la conexión y tipo de Interfaz del dispositivo que se conecta a las redes, será un RJ45 para enlaces de cobre o algún *transceiver* si se trata de fibra óptica. Es importante destacar que ambos extremos son del mismo tipo de conector.

Estos enlaces trabajan hasta capa de enlace. Trabajan bajo el estándar **IEEE 802.3** de Ethernet y el **IEEE 802.1q** de etiquetado por VLAN[1], pues el proveedor de servicios transporta los datos marcados.

[1] El concepto de VLAN se tratará más adelante.

1.1.2.2 Clasificación por cobertura

Esta clasificación de las redes de datos por cobertura depende del alcance que tienen las mismas con sus usuarios, es decir, el tamaño del área que cubren. Como una clasificación inicial están las redes de área personal, que como su nombre lo indica, son para una persona. Delante de esas redes se encuentran las redes de rango grande, estas pueden ser divididas en redes de área local, de área metropolitana y de área amplia. Finalmente la conexión de dos o más redes WAN (también llamadas *internetwork*s) es llamada *Internet*. En la figura 1.1 se puede observar esta clasificación debida a la cobertura.

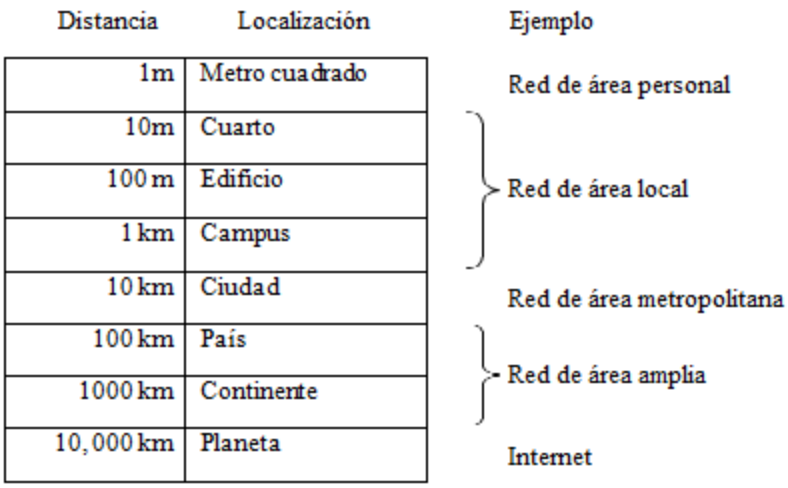

Figura 1.1. Clasificación de computadoras conectadas por escala.

Redes de Área Personal (PAN, Personal Area Networks)

Permite a los dispositivos comunicarse sobre el rango de una persona. Un ejemplo común es una red inalámbrica que conecta a una computadora con su periferia. Con lo que cuenta el dispositivo del usuario es monitor, teclado, ratón e impresora. Una ejemplo de este tipo de red es Bluetooth/WPAN que se especifica en el estándar **IEEE 802.15**.

Redes de Área Local (LAN, Local Area Networks)

Una red de este tipo está administrada por una sola organización. Son redes pequeñas que se encuentran en una única ubicación geográfica, como un edificio, una oficina o una fábrica. Las redes LAN son usadas ampliamente para conectar computadoras personales y dispositivos electrónicos para permitirles compartir recursos e intercambiar información. Cuando estas redes son usadas por compañías, son llamadas redes empresariales.

Las redes LAN inalámbricas (WLAN) son muy populares estos días, especialmente en casas, edificios de oficinas viejas, cafeterías y otros lugares donde es demasiado difícil instalar cableados. En estos sistemas cada computadora tiene un radio o una antena que utiliza para comunicarse con las otras a través de un dispositivo central llamado módem, punto de acceso o Router inalámbrico. Todos estos dispositivos usan el estándar **IEEE 802.11**.

Las redes LAN alámbricas usan diversas tecnologías de transmisión, como cables de cobre o fibra óptica. Corren velocidades de entre 100 Mbps a 1 Gbps y se caracterizan por tener un retardo de transmisión bajo. Las topologías de estas redes pueden estar conectadas por medio de enlaces punto a punto. El estándar usado es el **IEEE 802.3** llamado Ethernet. Para la conexión de estas redes se utilizan redes basadas en switches. En la figura 1.2 se puede observar la cobertura de este tipo de red.

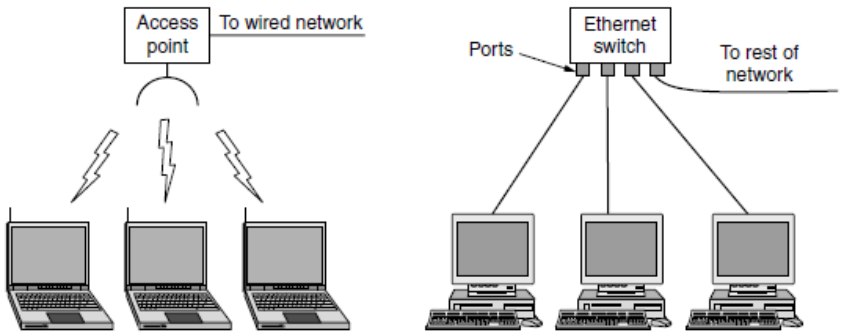

Figura 1.2. LAN inalámbrica (802.11) y LAN cableada (802.3).

Redes de Área Metropolitana (MAN, Metropolitan Area Networks)

Una red MAN cubre una ciudad. Un ejemplo muy bien conocido de este tipo son las redes de televisión por cable disponibles en muchas ciudades, que desde su origen se volvieron populares y debido a la demanda, se crearon contratos para el cableado entero de ciudades.

La televisión por cable no es la única red MAN. Desarrollos recientes de accesos de Internet inalámbricos de alta velocidad han resultado en otra MAN, estandarizados como IEEE 802.16 y que es conocido popularmente como **WiMAX**, y se ilustra en la figura 1.3.

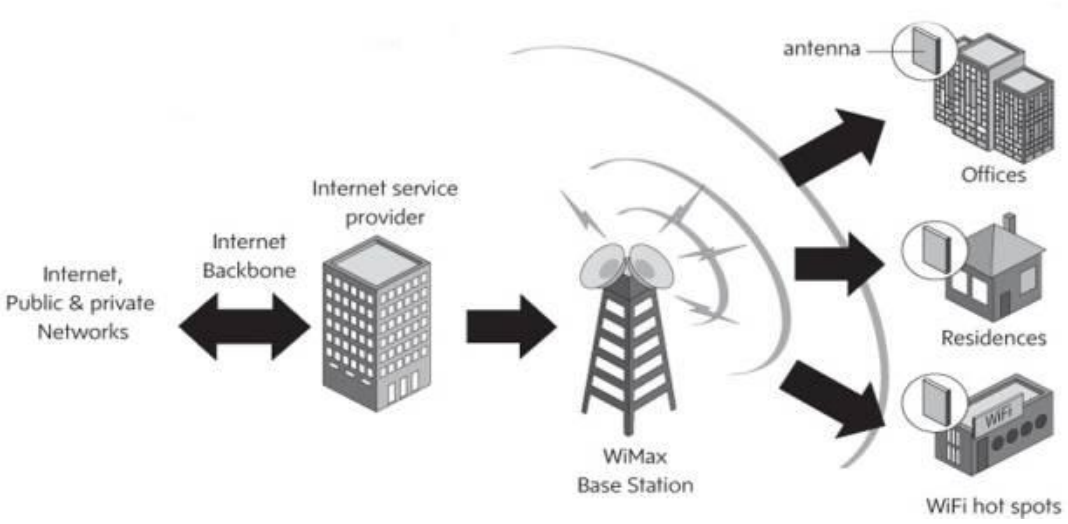

Figura 1.3. Una red MAN para el servicio de TV por cable.

Redes de Área Amplia (WAN)

Cuando una organización cuenta con diversas ubicaciones separadas por grandes distancias geográficas, desde un país a un continente, se conoce como red WAN y conecta entre sí a todas las redes de área local que componen dicha institución, tal como se puede apreciar en la figura 1.4. Esas redes LAN se conectan a través de la infraestructura que pertenece a un Proveedor de Servicios de Internet (*ISP, Internet Service Provider*), que se encarga de transportar los mensajes de LAN a LAN.

Los dispositivos de la red WAN puede ser descrita como una red LAN cableada gigante; sin embargo, hay algunas diferencias importantes que están detrás de esos grandes extensiones de cables. Usualmente en una WAN, las redes LAN y la infraestructura son operadas por diferentes personas, ya que las reglas y políticas que tiene la institución sobre sus redes locales serán gestionadas por ella misma, mientras que las políticas de la red que conecta a las redes las mantendrá el ISP.

Figura 1.4. Red WAN que conecta varios nodos de una organización.

Internet

Muchas redes existen en el mundo, a menudo con diferente hardware y software. Las personas conectadas a una red desean comunicarse con personas en diferente lugar. Para el cumplimiento de este deseo requiere que diferentes e incompatibles redes estén conectadas. La colección de redes interconectadas es llamada Internet. Internet usa redes de Proveedores de Servicio ISP para conectar redes empresariales, redes caseras y muchas más otras redes.

1.1.2.3 Clasificación por topologías

La tipología de una red de datos se refiere a la organización física de los dispositivos y su conexión a través de los medios de transmisión. Esto provoca que cada una de las diferentes topologías funcione de manera diferente y a su vez utilice métodos distintos que garanticen su buen funcionamiento y eviten la pérdida de la información durante su transmisión.

A continuación se explicarán las principales topologías utilizadas en las redes de datos, de estás derivan otras con mayor complejidad.

Topología Estrella

Es una topología utilizada desde 1960. En esta, cada uno de los dispositivos que compone la red está conectado a un dispositivo central, conocido como Router de señal o MAU (Unidad del acceso Multiestación) que repite o emite mensajes de control y de información logrando intercambiar mensajes a determinados dispositivos. Esa conexión se puede apreciar en la figura 1.5.

Esta topología es ideal para cualquier aplicación en la que múltiples rutas entre varios dispositivos son deseadas. Además, cuando uno de los dispositivos simples falla, el resto de los equipos no se verán afectados. Por el contrario, si el dispositivo central falla, todas las comunicaciones en la red fallarán.

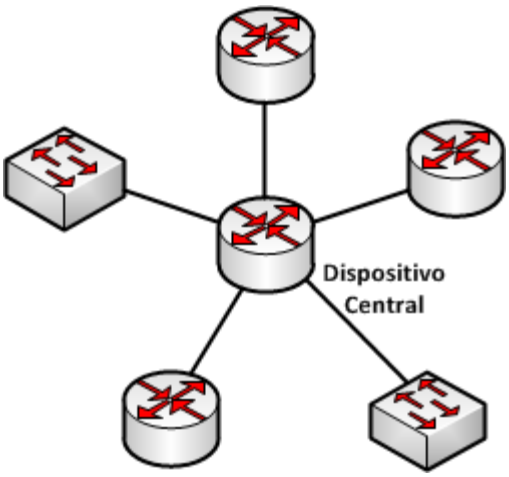

Figura 1.5. Topología estrella

Topología Bus

La topología de bus es un esquema simple en el que todos los dispositivos están conectados a un enlace común, además, todos los nodos en esta red tienen la misma jerarquía tal como aparece en la figura 1.6.

Por razones eléctricas, esta topología es usada en muchos estándares de control unidireccionales, donde se crea una conexión en cadena a través de todos los equipos con el dispositivo final terminando en línea. Esta topología puede ser encontrada dentro de computadoras personales, conectando expansiones internas y dispositivos periféricos. Los sistemas que usan la topología son fáciles de cablear pero tiene limitaciones en la distancia debido a que la señal que transmite los datos a lo largo del medio no es amplificada ni repetida como sea necesario.

Si ocurre alguna falla en cualquiera de los dispositivos de la red, esta sigue funcionando sin problemas, en cambio, si el medio de transmisión falla, la red entera dejará de funcionar.

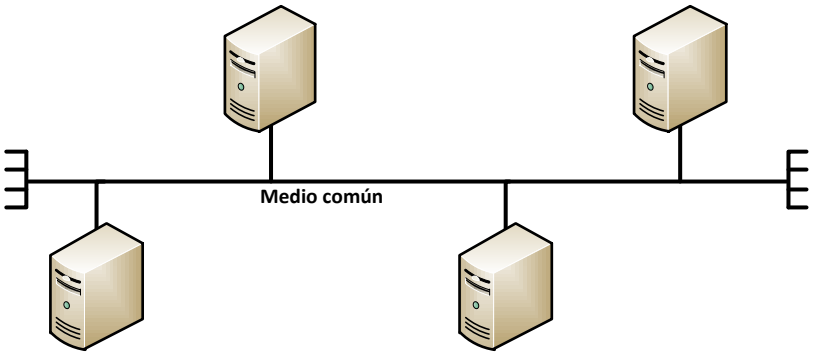

Figura 1.6. Topología Bus

Topología Anillo

En esta topología los dispositivos se conectan a la red en ciclo como se puede notar en la figura 1.7. Los datos son transportados de un equipo a otro alrededor de la secuencia de anillo. Esta topología cubre mayores distancias que otras, ya que los datos son amplificados y repetidos durante su paso alrededor del anillo. Sin embargo, una desventaja se hace presente cuando falla un dispositivo o un grupo de dispositivos que puede provocar la caída del

sistema completo porque se hace presente un punto que no repetirá la información. Asimismo, si falla el medio de transmisión, la red fallará. Una desventaja más es la dificultad para añadir nuevos dispositivos a la red después de la instalación inicial, ya que la red es cerrada.

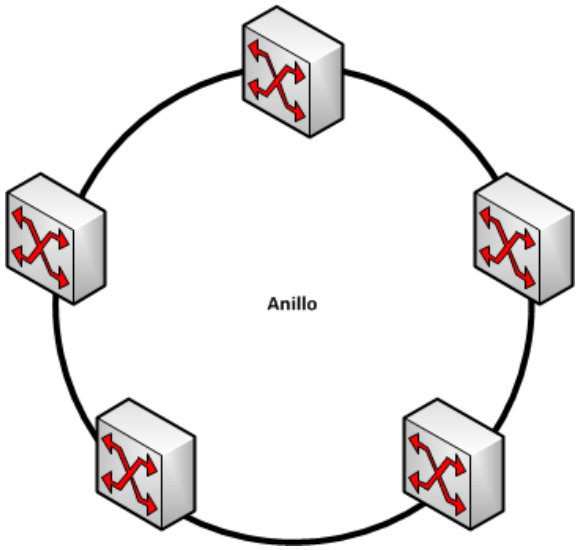

Figura 1.7. Topología anillo

Topología de Malla

La topología de malla se utiliza cuando los servicios que componen la red se encuentran dispersos geográficamente y se necesita un acceso fiable a ellos. Esta topología conecta cada uno de los dispositivos con los demás en la red, tal como la figura 1.8. Esta conexión se realiza por medio de enlaces físicos dedicados o por medio de enlaces virtuales. Esta topología ofrece gran redundancia, por lo que su implementación es costosa y su uso es amplio en las redes WAN.

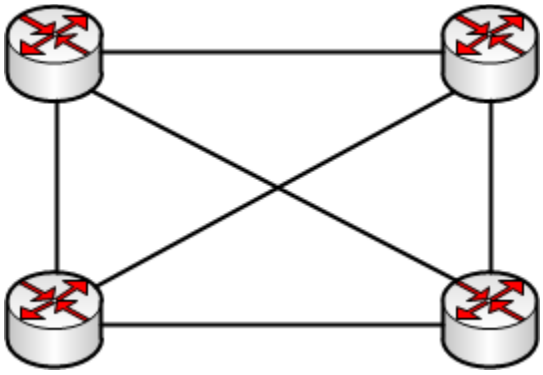

Figura 1.8. Topología malla

1.1.3 Estandarización de las redes de datos

Los organismos internacionales de estandarización entre sus actividades primarias son el desarrollo, la coordinación, la promulgación, la revisión, la reedición, la interpretación o la producción de algún estándar técnico que tienen por objeto atender las necesidades a problemas presentados por falta de compatibilidades.

Muchos proveedores de dispositivos de red tienen sus propias ideas para la realización de las cosas. Sin la coordinación adecuada, la comunicación se convierte en un caos completo y los usuarios son los afectados. La única manera para crear acuerdos de funcionamiento son los estándares. Los buenos estándares no sólo permitirán la comunicación entre dispositivos, sino que incrementa la venta de los dispositivos que están apegados a las normas, permitiendo mejores implementaciones, decrementos de precios e incremento de la aceptación de los productos.

Los estándares definen qué es necesario para la interoperabilidad, ni más ni menos. Son los que permiten a los mercados grandes emerger y permitirle a las compañías competir en base a qué tan servibles son sus productos. Por ejemplo, el estándar 802.11 define cuantos radios de transmisión existen; sin embargo, no dice cuando un transmisor utiliza cierto radio, factor clave para un buen desempeño. Esto depende de quién fabrica el producto. De esta forma obtener la interoperabilidad es difícil, en el que hay diversas elecciones y estándares que manejan muchas opciones. Para el estándar 802.11 hay muchos problemas que ha provocado que el grupo llamado **WiFi Alliance** trabaje en la interoperabilidad del estándar.

De manera similar, un protocolo estándar define el protocolo sobre el cable de conexión y no la interfaz del servicio dentro del dispositivo, excepto para ayudar a explicar el protocolo. Interfaces de servicio reales a menudo son propietarios. Por ejemplo, para una comunicación de TCP/IP para comunicar una computadora con un host remoto no importa. Lo único que importa es que el equipo remoto hable TCP/IP. De hecho, TCP e IP son comúnmente implementados juntos. Asimismo, los protocolos establecen el formato de los mensajes que se transmitirán y las reglas que se llevarán a cabo para que la comunicación se lleve a cabo.

Los estándares se clasifican en dos categorías: *de facto* y *de jure*. Los estándares **de facto** ("de hecho") son aquellos que han sido desarrollados sin ningún plan formal. HTTP, el protocolo que utiliza la Web inició su vida como un protocolo de facto. Era parte de los primeros navegadores web desarrollados por Tim Berners-Lee en CERN y su uso se hizo extenso con el crecimiento de la red. Bluetooth es otro ejemplo, fue originado por Ericsson, pero su uso se extendió a varios dispositivos.

Los estándares **de jure** ("por ley"), en contraste con los anteriores, son adoptados a través de las reglas de algún organismo oficial de estandarización. Las autoridades internacionales de estandarización están divididas generalmente en dos clases: aquellos establecidos por un tratado entre los gobiernos nacionales y aquellas organizaciones no gubernamentales voluntarias. En el ámbito de los estándares para las redes de datos hay varias organizaciones, en particular la ITU, ISO, IETF y la IEEE que serán discutidas más adelante.

En la práctica, es muy complicada la relación entre estándares, compañías, y organismos oficiales de estandarización. Estándares de facto a menudo se convierten en estándares de jure, especialmente si estos son muy exitosos, como ocurrió con HTTP, que rápidamente fue tomado por el IETF.

1.1.3.1 ITU (Unión Internacional de Telecomunicaciones)

Con todos los diferentes proveedores de servicios de telefonía y de Internet en todos los países, es necesario proveer compatibilidad a nivel mundial que garantice que las personas (y computadoras) en un país puedan comunicarse con su contraparte en otro sin problemas. En 1865, representantes de los gobiernos de Europa se reunieron para formar al predecesor de del ITU de hoy en día. Su trabajo fue estandarizar las telecomunicaciones internacionales, que en esos días se llevaba a cabo por medio de la telegrafía ya que la mitad de los países usaba código Morse, mientras que

los demás utilizaban otros códigos que se fueron convirtiendo en un problema para la comunicación. Cuando nació la telefonía como un servicio internacional, ITU tomó el trabajo de estandarizarla. En 1947, se convirtió en una agencia de las Naciones Unidas.

La ITU cuenta con alrededor de 200 miembros gubernamentales, incluyendo a casi todos los miembros de las Naciones Unidas

Cuenta con tres sectores principales, el primero de ellos se enfoca principalmente en **ITU-T**, el sector de la estandarización de las telecomunicaciones en lo que concierne a telefonía y sistemas de datos comunicación de datos. Antes de 1993 este sector era llamado CCITT, que es el acrónimo de su nombre en francés. El sector de las radiocomunicaciones **ITU-R**, se encarga de la coordinación de uso de las frecuencias de radio de todo el mundo por los grupos de interés. El otro sector es el **ITU-D**, llamado sector de desarrollo. Este último promueve el desarrollo de tecnologías de la información y comunicaciones para la reducción de la "brecha digital" que existe entre los países de acceso efectivo a las tecnologías de la información y de los países con acceso ilimitado.

1.1.3.2 ISO (Organización Internacional para la Estandarización)

Los estándares internacionales son producidos y publicados por la ISO, una organización voluntaria no gubernamental que surgió en 1946. Sus miembros son autoridades nacionales de estandarización de 157 países. Entre esos miembros se incluyen ANSI (EUA), BSI (Gran Bretaña), AFNOR (Francia), DIN (Alemania) y otras 153.

Existen un gran número de normas emitidas por la ISO que abarcan un gran número de temas. Por ejemplo, postes telegráficos (ISO 2451), redes de pesca (ISO 1530) entre otros, con la finalidad de coordinar las normas en cada país, facilitando el comercio y su contribución a las normas de desarrollo. ISO es miembro de ITU-T y a menudo cooperan para evitar que se desarrollen estándares mutuamente incompatibles.

1.1.3.3 IEEE (Instituto de Ingenieros Eléctricos y Electrónicos)

La IEEE es la organización profesional más grande del mundo. Además de sus decenas de revistas y conferencias cada año, cuenta con un grupo de profesionales que desarrollan estándares en el área de la ingeniería electrónica y la computación. El comité 802 de la IEEE ha estandarizado muchos tipos de redes LAN por ejemplo.

1.1.3.4 IETF (Fuerza de Tareas de Ingeniería de Internet)

Después de la puesta en operación de ARPANET, el Departamento de Defensa de Estados Unidos creó un comité informal para su supervisión, y en 1983 fue llamado IAB (Consejo de Actividades de Internet) a la que se le dio la tarea de la realización de las investigaciones relacionadas con ARPANET e Internet en la misma dirección. El significado del acrónimo "IAB" cambio más tarde por Consejo de Arquitectura de Internet.

Cuando un estándar era necesario (por ejemplo, un nuevo algoritmo de enrutamiento), miembros de la IAB anunciaban el cambio a estudiantes graduados de universidad para su implementación. Esa comunicación generó una serie de reportes técnicos llamados RFCs (Solicitudes de comentarios) que se encuentran almacenados en línea y son de acceso a cualquier interesado en conocerlos a través del sitio *www.ieft.org/rfc*. Están numerados por orden cronológico de creación. Alrededor de 5000 documentos RFC existen ahora.

En 1989, la IAB fue reorganizada, que en ese momento supervisaba varios "grupos de trabajo", dejándole sólo dos, la IETF y la IRTF (Fuerza de Tareas de Recursos de Internet). Actualmente la IETF cuenta con una comunidad internacional abierta de diseñadores de red, operadores, compañías e investigadores interesados en la evolución de la arquitectura de Internet y su operación.

El actual trabajo técnico del IETF es hecho por sus grupos de trabajo, que están organizados en varias áreas (por ejemplo, enrutamiento, transporte, seguridad, etc.), además de que se mantienen tres reuniones por año.

La Autoridad de Asignación de Números de Internet (IANA) es el coordinador central para la asignación de parámetros únicos para los protocolos de Internet. La IANA está constituida por la Sociedad de Internet (ISOC) que actúa como centro de información para la asignación y coordinación del uso de numerosos parámetros de Internet.

1.1.3.5 El modelo de referencia OSI

El modelo OSI es una propuesta elaborada por la Organización Internacional de Estandarización (ISO) como primer paso para la normalización de los protocolos utilizados en la comunicación en las redes de datos. Fue revisado en 1995 y fue llamado modelo de referencia ISO OSI (Interconexión de Sistemas Abiertos) porque se trata de la conexión de sistemas abiertos con otros sistemas.

El modelo OSI cuenta con siete capas (figura 1.9). En este modelo tiene principios que fueron aplicados para llegar a él y se resumen brevemente como sigue:

- Una capa puede ser creada donde una abstracción diferente es necesaria.
- Cada capa debe de tener una función bien definida.
- La función de cada capa puede ser elegida hacia la definición de protocolos internacionales estandarizados.
- Los límites de la capa pueden ser elegidos para minimizar el flujo de información a través de las interfaces.
- El número de capas puede ser lo suficientemente grande para que las diferentes funciones necesarias no se encuentren en una misma capa y suficientemente pequeño para que la arquitectura no se convierta difícil de administrar.

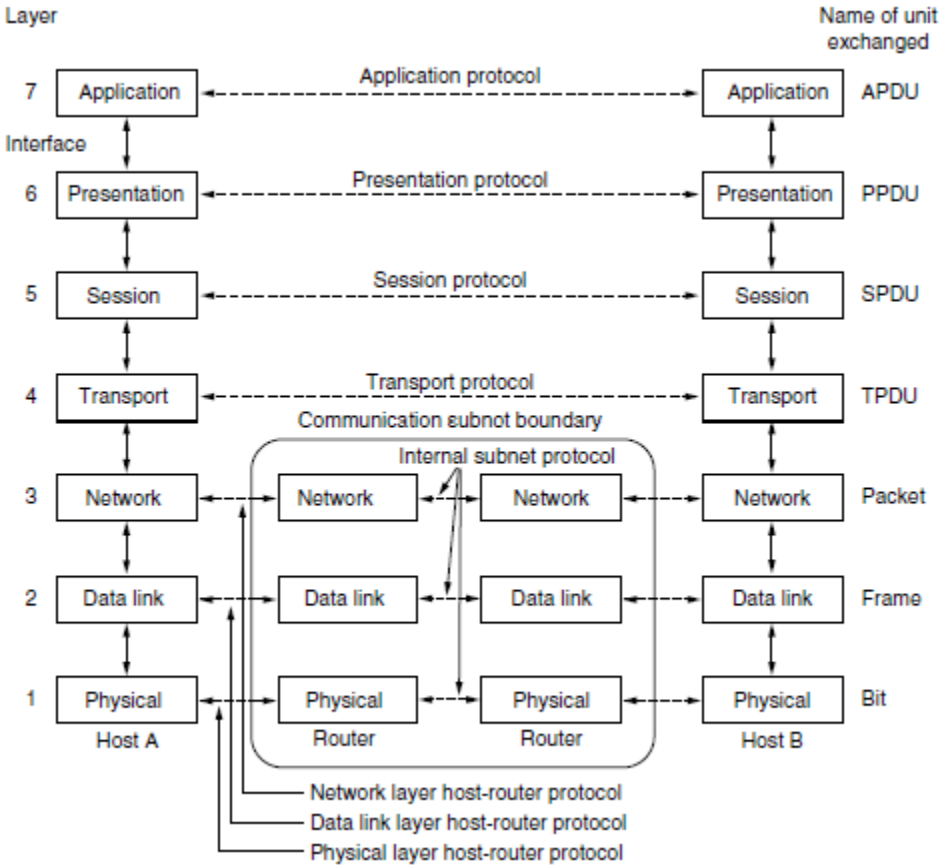

Figura 1.9. Modelo de referencia OSI

Los principios de cada capa se pueden resumir brevemente de la siguiente manera:

Capa 1 Física

Es la encargada de la transmisión de bits a través de un canal de comunicación. Describe los medios mecánicos, eléctricos, funcionales y de procedimientos que son utilizados para activar y desactivar conexiones físicas para la transmisión de bits hacia y desde un dispositivo de red. Se debe de garantizar que cuando se envía un 1, en el extremo también sea un 1 y no un 0.

Se toma en cuenta la velocidad de transmisión que tendrá cada medio, así como la presencia de la probabilidad del error en la transmisión, siendo la primera de ellas un tópico que no se puede manejar fácilmente ya que depende de cada medio y sus características; sin embargo, la probabilidad de error se puede corregir por medio de algoritmos y los protocolos de la capa.

Capa 2 Enlace

Esta capa se encarga de asegurar la fiabilidad de la transmisión de datos entre los nodos involucrados en la comunicación. Se describen los métodos utilizados para el intercambio de tramas a través de un medio común.

Existen dos tareas importantes en esta capa, la primera de ellas es el control de acceso al medio la cual depende de la topología lógica y el medio físico para determinar el método de acceso a los medios a utilizar. La segunda terea es la detección y corrección de errores, en la cual se implementan mecanismos tales como la adicción de bits al mensaje original para poder hacer verificaciones y pedir una retransmisión en caso de ocurrir algún fallo.

Capa 3 Red

Esta capa proporciona los servicios para el intercambio de datos en la red entre los dispositivos finales identificados. Para lograr esa comunicación lleva a cabo cuatro procesos básicos de importancia: direccionamiento, encapsulación, ruteo y desencapsulación, tareas que son llevadas a cabo por el dispositivo llamado Router.

Capa 4 Transporte

La capa de transporte se encarga de preparar los datos de las capas superiores para transportarlos a través de la red y realizar el procesamiento de los datos para su utilización por las aplicaciones.

Entre las responsabilidades de esta capa están: rastreo de las diferentes comunicaciones establecidas entres los dispositivos origen y destino, segmentación y manejo de cada una de las partes, reensamble de los segmentos en streams de datos para cada aplicación y la identificación de las diferentes aplicaciones por medio de puertos.

Los protocolos más utilizados de esta capa son TCP y UDP:

- TCP (Protocolo de Control de Transferencia): Es un protocolo de transporte usado en la mayoría de los servicios de Internet para la realización de conexiones entre hosts a través de las redes. Utiliza recursos adicionales que le permiten adquirir funciones para lograr que los segmentos que componen un mensaje lleguen en orden, de manera confiable, además de ofrecer control de flujo. Este protocolo funciona en conjunto con el protocolo de *Enlace de tres vías*, encargado de establecer una sesión entre los host involucrados en la comunicación, y haciendo el uso de "Acuses de recibo" o mensajes ACK. Este mecanismo permite que durante la comunicación los mensajes lleguen completos y sin modificación, y en caso de haber un fallo se solicita su retransmisión. El uso de los recursos adicionales se da debido a los acuses de recibo por cada mensaje que se ha enviado, así como las retransmisiones, que proporcionan confiabilidad.

  Aplicaciones que utilizan éste conexiones usando este protocolo se encuentran el envío de correo electrónico, los navegadores web y la transferencia de archivos.

- UDP (Protocolo de Datagramas de Usuario): Es un protocolo de transporte orientado a no conexión. Este protocolo intercambia datagramas sin el envío de acuses de recibo ni garantía de que se han enviado, el envío no se da en orden por lo que el procesamiento de errores, solicitud de retransmisión en caso de haber pérdidas y reensamblaje de mensajes es implementado por otros protocolos.

Capa 5 Sesión

La capa de sesión proporciona los servicios a la capa de presentación para administrar las conexiones, la recuperación de las pérdidas de comunicación y la gestión del intercambio de datos.

Capa 6 Presentación

Esta capa se encarga de definir una forma estándar de la codificación y presentación de la información, así como cualquier conversión que se necesiten entre los diferentes formatos existentes. Dicha codificación puede poseer propiedades de eficiencia (compresión) o de seguridad (cifrado).

Capa 7 Aplicación

En esta capa se presentan los programas y servicios que permiten al usuario interactuar con la red de manera fácil y que trabajan siguiendo un modelo extremo a extremo entre los individuos que utilizan la red.

Entre los protocolos más populares en esta capa están:

- DNS (Sistema de Nombres de Dominio): Este protocolo se encarga de traducir nombres de dominio (direcciones web que representan un host) a sus respectivas direcciones IP.
- HTTP (Protocolo de Transferencia de Hipertexto): Es el método utilizado para la transferencia y transmisión de información en la World Wide Web.
- FTP (Protocolo de Transferencia de Archivos): Utilizado en la transferencia de archivos entre sistemas de red conectados.
- DHCP (Protocolo de Configuración Dinámica de Host): Es un protocolo utilizado para solicitar y asignar direcciones IP, dirección del equipo de salida y dirección de servidor DNS en caso de haber uno configurado.
- SMTP (Protocolo Simple de Transferencia de Correo): Protocolo utilizado para las transmisiones de mensajes de correo electrónico a través de Internet.

1.1.3.6 El modelo de referencia TCP/IP

La historia del modelo TCP/IP surge a partir de ARPANET que fue una red de investigación creada por el Departamento de Defensa de los Estados Unidos (DoD). Esta red eventualmente conectó a cientos de universidades e instalaciones gubernamentales usando líneas telefónicas arrendadas. Cuando las redes satelitales y de radio se añadieron, empezaron a existir problemas con los protocolos que interconectaban a las redes originando la necesidad de generar una arquitectura de referencia. El principal objetivo de diseño de esta arquitectura fue la conexión de múltiples redes de manera transparente en los inicios. Este modelo tiempo después se convirtió en el conocido Modelo de Referencia TCP/IP después del desarrollo de sus dos principales protocolos. Fue descrito por primera vez por Cerf y Kahn (1974) y después se redefinió y se convirtió en estándar en la comunidad de Internet en 1989.

Después de que el DoD se preocupó por la pérdida de parte de su infraestructura de red, entre ellos hosts, Routers y gateways debido al ataque de la Unión Soviética, otro de los mayores objetivos del modelo de referencia fue el de mantener a la red disponible a pesar de las pérdidas de hardware, y de la independencia de la creación de conversaciones previas. En otras palabras, el deseo del departamento de defensa era mantener las conexiones siempre y cuando la fuente de datos y el destino se mantuvieran intactos, a pesar que algunos de los dispositivos de

transmisión intermedios se hayan perdido. Asimismo, la necesidad de aplicaciones que permitieran la transmisión de archivos y de voz en tiempo real requirió de una arquitectura flexible.

Capa de acceso a la red

Esta capa define los protocolos y hardware requerido para entregar los datos a través de la red física. El término de acceso a la red se refiere al hecho de que la capa define cómo se conectan físicamente los dispositivos al medio de físico sobre qué datos pueden ser transmitidos. Por ejemplo, Ethernet es un ejemplo de protocolo de esta capa. Ethernet define el cableado, direccionamiento y protocolos a utilizar para crear una LAN. Asimismo, se determinan los protocolos para la creación de redes WAN.

La capa de acceso a la red incluye los protocolos, estándares de cableado y cabeceras que definen cómo se enviarán los datos a través de una amplia variedad de tipos de redes físicas.

Capa de Internet

La capa de Internet del modelo TCP/IP está definido principalmente por el Protocolo de Internet IP. Este protocolo define que el direccionamiento de cada uno de los hosts debe de ser diferente. Asimismo, se define el proceso de ruteo en los dispositivos llamados Routers que eligen a dónde enviar los paquetes

Capa de Transporte

La capa de transporte consiste principalmente en dos protocolos, el Protocolo de Control de Transmisión (TCP) y el Protocolo de Datagramas de Usuario (UDP). El primer protocolo de ellos se encarga de la creación de comunicaciones sin pérdida de paquetes, pues se trata de un protocolo orientado a conexión que integra un mecanismo para garantizar la recuperación de errores por medio de mensajes de acuse de recibo (*acknowledgments*). Este protocolo divide los datos en segmentos para su transmisión, pero en la recepción, este mismo protocolo se encarga del reensamblaje de la información. Además, se establece un control de flujo para controlar los envíos de datos en caso de que el destino no tenga la capacidad de procesar la cantidad de datos que se le envían,, controlando la cantidad de datos enviados.

En cambio, el protocolo UDP no está orientado a conexión, por lo que permite la pérdida de segmentos durante la transmisión de los datos ya que no existe un mecanismo de recuperación de errores. Debido a esta característica, las comunicaciones por medio de este protocolo son rápidas.

Capa de Aplicación

Esta capa provee servicios al software de aplicación que se ejecuta en las computadoras. Esta capa no define a la aplicación misma, pero define los servicios que esta necesita, como la transferencia de archivos para HTTP. En pocas palabras, la capa de aplicación provee una interfaz entre el software que está funcionando en una computadoras y su interacción con la red.

1.1.4 Elementos de una red de datos

Una red de datos se compone de varios dispositivos que hacen posible que las organizaciones gubernamentales, educativas, de investigación y compañías se comuniquen entre si y compartan recursos. Para los usuarios finales, la única interfaz que tendrán como acceso a la red será su estación de trabajo y las aplicaciones que ejecuten para interaccionar, usualmente un navegador web. Sin embargo, hay toda una infraestructura de dispositivos de los cuales no son visibles por el usuario. Estos dispositivos están interconectados y utilizan protocolos y estándares para la transmisión de la información de un lugar a otro. Ejemplo de estos dispositivos se encuentran los siguientes:

- Dispositivos de acceso a la red (hubs, switches y puntos de acceso inalámbricos)
- Dispositivos de Internetwork (Routers)
- Servidores y dispositivos finales
- Dispositivos de seguridad (firewalls)

Estos dispositivos permiten la administración de la información entre otras funciones. Tienen asignada una dirección de red que permite su administración e identificación a través de la red. Asimismo se encargan de garantizar la comunicación entre dos dispositivos finales, así como de proporcionar una ruta a la información para que legue a su destino. Entre otras de las funciones principales de estos dispositivos se encuentran:

- Generación y transmisión de señales que representan los datos.
- Conservar información acerca de las rutas a utilizar para llegar a cierto destino.
- Detección y notificación de fallas de algún dispositivo en la red.
- Clasificación de la información según la prioridad con la que hay sido clasificados los datos.
- Permitir o denegar cierto flujo de información según la configuración de los parámetros de seguridad.

A continuación se proporciona una descripción y características de los principales dispositivos intermedios:

1.1.4.1 Router

El Router se puede identificar como una computadora con sistema operativo y un hardware especializado para el ruteo de paquetes. Sus elementos de hardware son las siguientes: CPU, memorias RAM (Memoria de Acceso Aleatorio), memoria ROM (Memoria de Sólo Lectura), memoria flash y memoria NVRAM (Memoria de Acceso Aleatorio No Volátil).

Es un dispositivo intermedio que tiene como tarea la de interconectar a diversas redes de datos. Por esa misma razón, están compuestos por varias interfaces, y cada una de ellas pertenece a una red IP diferente. Las redes que interconecta un Router son Redes de Área Local (LAN) entre las que se encuentran redes empresariales, domésticas y establecimientos, y la conexión de Redes de Área Extensa (WAN) para la conexión de redes a través de un área geográfica extensa. De esta manera se tienen los siguientes tipos de interfaces:

- Interfaces comunes para interconexión de redes:
    - Puertos FastEthernet y GigabitEthernet

Las interfaces FastEthernet, GigabitEthernet y TenGigabitEthernet son utilizadas para conectar redes LAN (en el caso de las interfaces FastEthernet) o para la realización de enlaces entre nodos (por medio de las interfaces GigabitEthernet o/y TenGigabitEthernet). Va a depender de la topología y lo que se desea conectar para determinar el tipo de interfaz a utilizar, ya que cada una de estas ofrece una velocidad diferente una de las otras.

Este tipo de interfaces regularmente vienen acompañados por un cable de conector de RJ-45, sin embargo, algunos dispositivos ya aceptan enlaces de este tipo con medio de fibra óptica, conectores necesarios, entre otras.

Las velocidades de este tipo de enlaces es el siguiente:

- FastEthernet: 100Mbps.
- Gigabit Ethernet: 1000Mbps

- Puertos Seriales

Estás interfaces son conocidas con WAN, ya que a través de estás es posible realizar la conexión entre dispositivos separados a gran distancia. Se pueden observar los diferentes tipos de conectores seriales que existen en la figura 1.10.

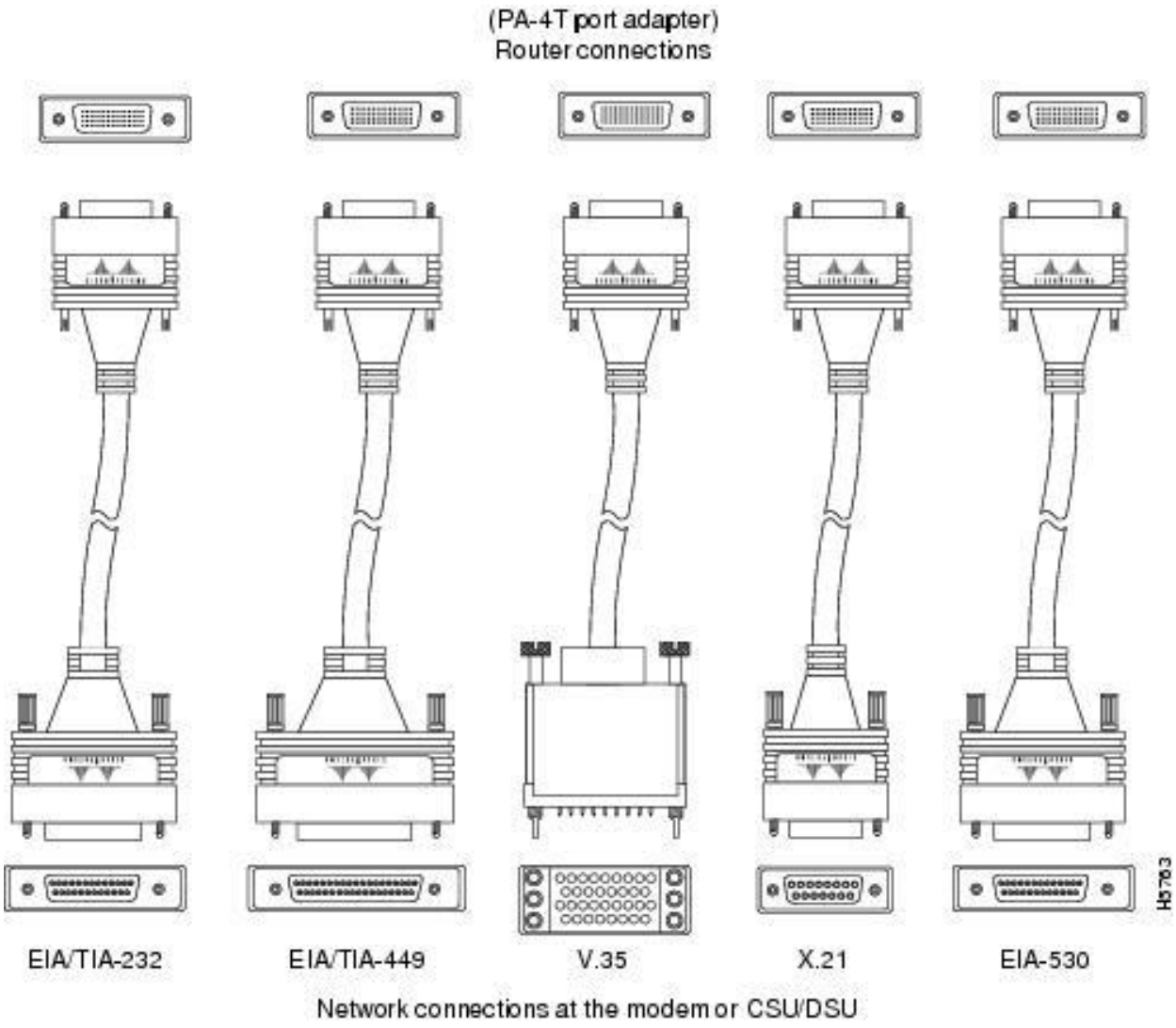

Figura 1.10. Interfaces seriales.

- Interfaces para la administración y configuración del dispositivo:
  - Puerto consola

El puerto de consola es utilizado para la configuración del equipo conectado directamente a la misma para la realización de cierta actividad de configuración o de consulta en el equipo, como en la figura 1.11. Esta conexión tiene que ser configurada correctamente a través de una aplicación en el dispositivo del administrador para el correcto despliegue de la información por parte del Router. Entre los parámetros a configurar se encuentran la tasa de transmisión (bits por segundo), la cantidad de bits de datos, el tipo de paridad, los bits de parada y el tipo de

control de flujo que se requiere. Estos parámetros pueden ser diferentes según el tipo de dispositivo de red, fabricante y modelo.

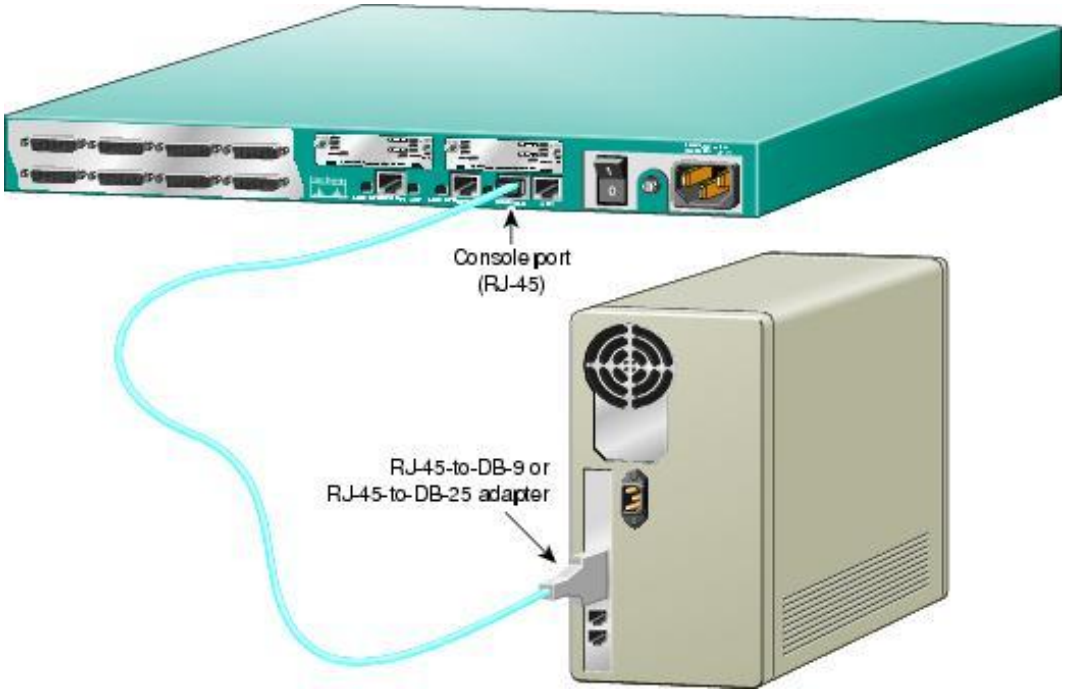

Figura 1.11. Conexión de un Router a una computadora a través de su puerto de consola.

Las interfaces para la conexión de redes pueden ser variadas y más de las que se mencionan aquí, depende del modelo del dispositivo, así como de los diferentes tipos de redes que se conectarán al dispositivo. Los puertos consola y auxiliar son utilizados por el administrador de la red para el control y configuración del dispositivo y de sus interfaces de red.

El Router tiene la capacidad de manejar datos del formato de las tres capas inferiores física, enlace de datos y de red, siendo la última de ellas la más importante, esto se debe a que su trabajo principal es la determinación de la mejor ruta y el reenvío de paquetes a su destino, por lo que el uso de direcciones IP es fundamental. Por esta misma razón, se dice que este dispositivo es de capa 3.

Las dos funciones principales del Router son:

- ***La determinación del mejor camino para reenvío de paquetes***: Esto se consigue compartiendo información de rutas entre los Routers y con ésta se completarán las tablas de ruteo haciendo el uso de algoritmos según el protocolo configurado, determinando las mejores rutas para ofrecer opciones para que se realice la transmisión de información durante la comunicación.
- ***El reenvío de paquetes a su destino***: Ya que los Routers en la red han compartido información acerca de las rutas a diferentes redes, las tablas de rutas son utilizadas para elegir el mejor camino para el envío de paquetes a redes externas. Se hace uso de las direcciones de red (IP) para identificar la ruta a seguir.

Los protocolos más frecuentemente utilizados en la determinación del mejor camino son los siguientes:

- ***RIP (Protocolo de Información de ruteo)***: Protocolo que utiliza un algoritmo *vector distancia* para la actualización de su tabla de ruteo, en particular el algoritmo Bellman Ford. Utiliza como métrica el conteo de saltos y las actualizaciones hacía otros Routers se envían por medio de segmentos UDP a través del puerto 520 cada 30 segundos con la tabla de ruteo completa a través de un envío broadcast.

- ***EIGRP (Protocolo de Gateway Interior Mejorado)***: Es un protocolo patentado y desarrollado por CISCO® de tipo *vector distancia* que utiliza el algoritmo de difusión (DUAL) para el envío de actualizaciones y construcción de la tabla de ruteo. La métrica utilizada por este protocolo es compuesta, y se utiliza el ancho de banda, el retardo, la carga y la confiabilidad. Se envían actualizaciones al detectarse un cambió en la topología de la red a través de envíos multicast y actualizaciones limitadas (sólo la información que cambió) utilizando el Protocolo de Transporte Confiable (RTP), no se utiliza TCP ni UDP debido a que este protocolo no sólo se implementa sobre redes IP, también es usado para redes IPX y Apple Talk.

- ***OSPF (Open Shortest Path First):*** Es un protocolo de ruteo Estado Enlace que hace uso del algoritmo shortest path first (SPF) de Dijkstra. La métrica que utiliza es el ancho de banda del canal y envía sus actualizaciones vía multicast. Hace uso de cinco tipos de paquetes para realizar el proceso de búsqueda de otros Routers, solicitar y envía información. Uno de los paquetes es utilizado como acuse de recibo en el envío de actualizaciones, por lo que no se utiliza ningún protocolo de transporte como TCP y UDP.

- ***IS-IS (Intermediate System To Intermediate System)***: Es un protocolo de ruteo de tipo *Estado Enlace* muy rápido en la convergencia de redes y con gran escalabilidad. El algoritmo de ruteo está basado en un método llamado DECnet fase V, en el cual Routers conocidos como sistemas intermediarios intercambian información de ruteo mediante una sola métrica para determinar la topología de la red. Este modelo fue desarrollado por la Organización Internacional de Estandarización (ISO) como parte del modelo de referencia OSI.

Estos son los protocolos de ruteo más utilizados y son conocidos como Protocolos de Gateway Interior (IGP) ya que son utilizados para intercambiar información de ruteo dentro de un sistema autónomo.

1.1.4.2 Switch

En la actualidad, muchos negocios con redes de datos utilizan Switches para conectar computadoras, impresoras y servidores que trabajan dentro de un edificio o campus. Este dispositivo no es utilizado para crear redes, el propósito principal es hacer más eficiente el trabajo de la LAN.

El uso del *Switch* en las redes de datos llegó a resolver varios problemas que habían traído consigo los *hubs*.

El *Hub* es un dispositivo que permite conectar dispositivos a un segmento de red de área local (LAN); sin embargo, no permite el filtrado de tráfico, en su lugar, envían todos los bits a todos los dispositivos de la red obligándolos a compartir el ancho de banda. Esto ocasiona que ocurran colisiones y provoque un bajo rendimiento de la red. Esto se debe a que se crea un dominio de colisiones, mientras más dispositivos se encuentran conectados a un dominio de colisiones, la red se vuelve ineficiente también, debido a que las colisiones entre las tramas generadas en la red son más frecuentes.

Una red de hubs no permite que las redes crezcan (escalabilidad) dado que al agregar un dispositivo más, el ancho de banda promedio por dispositivo disminuye. El tiempo que tardan las señales a llegar a los dispositivos (latencia) aumenta al expandir la longitud de los medios o al aumentar en número de dispositivos en la red. Además, dado que el medio es compartido y el Hub envía la información a todos los dispositivos conectados, si alguno de ellos está mal configurado y envía tráfico perjudicial, afectará gravemente a toda la red.

Por su parte, el Switch proporcionará un dominio de colisiones independiente por cada uno de sus puertos y un ancho de banda completo, nada es compartido como en el caso del Hub.

De esta manera, el Switch puede ser utilizado en dos casos particulares. Uno de ellos es actuar como dispositivo central entre dos hubs, compartiendo el ancho de banda aún, pero aislando los segmentos, por lo que se limitarán las colisiones. La otra forma de ser utilizado es conectando a cada puerto del Switch un nodo, el ancho de banda está dedicado a cada puerto, libre de colisiones y la operación es *full-dúplex.*

El Switch trabaja en la capa *2* del modelo OSI y posee la capacidad de detectar errores gracias al campo FCS (Frame Check Sequence) de las tramas Ethernet con las que trabaja. El reenvío de tramas se hace selectivamente desde un puerto transmisor al destino, esto se logra por medio de direcciones MAC, por este motivo se mantiene una tabla que hace coincidir cada una de estas direcciones con un puerto del dispositivo.

Las funciones básicas que realiza el Switch son las siguientes:

- ***Aprendizaje***: La tabla de direcciones MAC debe completarse, asociando cada una de las direcciones MAC del dispositivo al puerto correspondiente del Switch.
- ***Actualización***: Cada vez que se asocie una dirección MAC con un puerto del Switch, se la agregará una marca horaria, la cual se irá disminuyendo, al llegar a cero la entrada en la tabla se elimina, hasta recibir una trama en el puerto y agregar nuevamente.
- ***Saturación***: Cuando el Switch no tiene una entrada para una dirección MAC, este envía la trama a todos los puertos excepto por el cual llegó. A este proceso se le llama saturación.
- ***Reenvío selectivo***: Al recibir una trama, el Switch revisa la dirección MAC destino, analiza la tabla y se hace coincidir con una entrada, consecuentemente enviando la trama al puerto correspondiente.
- ***Filtrado***: No todas las tramas son reenviadas, en caso de que hayan sido dañadas se descartan, o por motivos de seguridad bloqueando tramas que se dirigen a ciertas direcciones MAC.

El trabajo del Switch se realiza más rápido que el de un Router en virtud de que no se modifica al paquete de datos, únicamente se lee la trama encapsulando el paquete, lo que hace que el proceso del Switch sea más rápido y menos propenso a errores. Otras características que ofrece son: velocidad del cableado, baja latencia y bajo costo.

Redes de Área Local Virtuales (VLAN)

Las Redes de Área Local virtuales (Virtual Area Local Networks, VLAN) son mecanismos que permiten a los administradores de red crear subredes a través de un Switch simple o un grupo de Switches independientemente de la proximidad física. Esta función es útil para reducir el número de dispositivos en los dominios de broadcast o permitir conjuntos de usuarios agrupados lógicamente sin la necesidad de estar localizados físicamente en el mismo lugar, aunque compartan la misma infraestructura.

Un dominio de broadcast es un conjunto de dispositivos en el que si alguno envía un mensaje de broadcast a los demás, todos los dispositivos dentro del mismo dominio lo recibirán. Así, si diversos dispositivos se encuentran en el mismo segmento de red, pueden recibir cualquier mensaje de broadcast generado en el mismo. El Switch en su configuración por default presenta un sólo dominio de broadcast, mismo dominio que puede afectar al desempeño de la red si existen diversos dispositivos conectados a ella. El dominio de broadcast en el Switch se puede segmentar en varios otros de pequeño tamaño gracias a la segmentación por VLAN, este está definido en el estándar **IEEE 802.1Q**.

Las VLAN pueden tener asignado un nombre para su fácil identificación al configurarse en el Switch, así como la de asignarle puertos. El dispositivo final (una PC, teléfono móvil o laptop) conectado en la VLAN debe de tener asignada una dirección IP de la subred de la VLAN.

En la figura 1.12 se tiene una red sin VLAN. En esta todos los dispositivos pertenecen al mismo dominio de broadcast, es decir, cuando un dispositivo envía un mensaje a la dirección de broadcast, todos los dispositivos en la red lo recibirán. Sin embargo, debido a las características del Switch que conecta a los dispositivos, cada máquina cuenta con su propio dominio de colisiones.

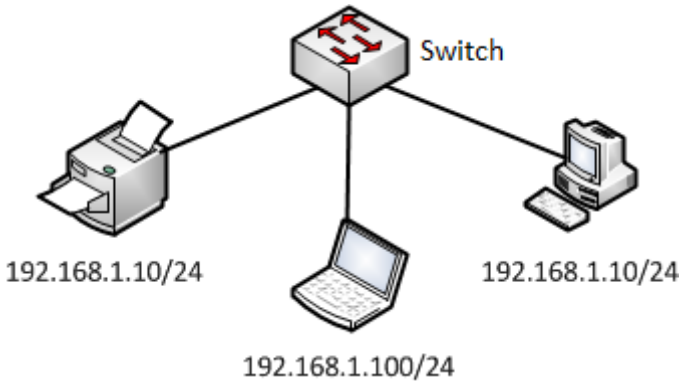

Figura 1.12. Red sin VLAN.

En la figura 1.13, en la red se tiene configuradas tres VLAN, cada una de ellas representa un dominio de broadcast independiente, y a su vez, se tratan de subredes diferentes a pesar de que todos los dispositivos se encuentran conectados en el mismo Switch.

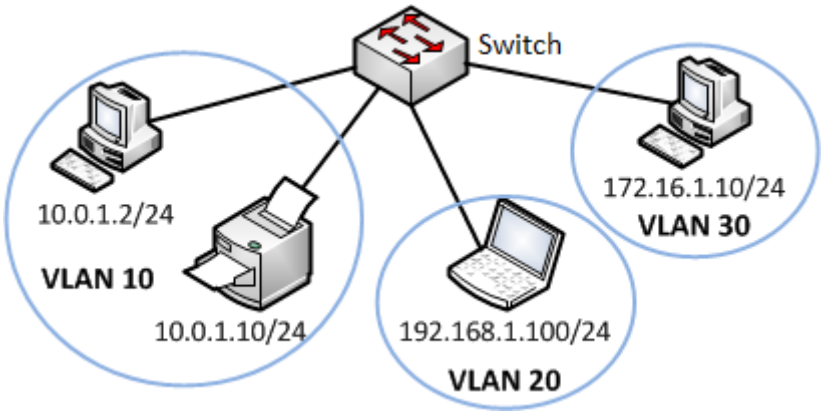

Figura 1.13. Red con VLAN.

Las VLAN proporcionan:

- **Seguridad:** los grupos permiten que la información sea separada del resto de la red disminuyendo la posibilidad de que ocurran violaciones a la confidencialidad.

- **Reducción de costos:** se hacen innecesarias las actualizaciones de red caras y el uso de los enlaces y el ancho de banda se hace presente.

- **Mejor rendimiento:** la división de la red en grupos lógicos reduce el tráfico innecesario en la red, así como la determinación de la Unidad Máxima de Transmisión (MTU) por VLAN.

- **Mitigación de la tormenta de broadcast:** las tormentas de broadcast ya no afectan a todos los dispositivos de la red, solo a aquellos que pertenecen a la VLAN correspondiente.

- **Administración de proyectos y aplicaciones simples:** la división en VLAN permite que grupos de usuarios con las mismas características de requerimientos compartan la red, asimismo, trabajar con proyectos o aplicaciones es más fácil, así como la de determinar el alcance de las actualizaciones de red.

Existen varios tipos de VLAN:

- VLAN nativa es aquella utilizada para la comunicación de dispositivos de una VLAN en diferentes Switches. La VLAN nativa tiene la capacidad de transportar tramas de diferentes VLAN a sus destinos. Ningún dispositivo pertenece a esta VLAN, sólo es utilizada para la comunicación entre dispositivos de una VLAN ubicados en diferentes Switches.

- VLAN de datos son aquellas utilizadas para la creación de grupos de usuarios.

- VLAN de voz es utilizada especialmente para el tráfico de voz en la red.

La comunicación de dispositivos de una VLAN a través de diferentes Switches hace uso de enlaces troncales. Un enlace troncal conecta diversos Switches en una red entre sí y permite el tráfico entre las diversas VLAN a través de un solo enlace físico y no por medio de varios enlaces dedicados para cada VLAN existente en la red a través de los Switches. El estándar IEEE 802.1Q que lo proporciona es llamado también *dot1q* o *protocolo de enlace troncal*.

En el caso de que no se utilizara un enlace troncal en la conexión de dos switches, se tendría que tener una conexión física por cada una de las VLAN en cada Switch.

Por ejemplo, en la figura 1.14 en la red existen tres VLAN, la 10, 20 y 30. Existen tres switches que tienen configuradas esas tres VLAN, y conectadas entre sí sin el uso de enlace troncal, se tendría que tener un enlace por cada una de ellas. Sin embargo, si se tiene un enlace troncal, basta con una sola conexión entre los switches para que exista la comunicación, tal es el caso de la imagen 1.15.

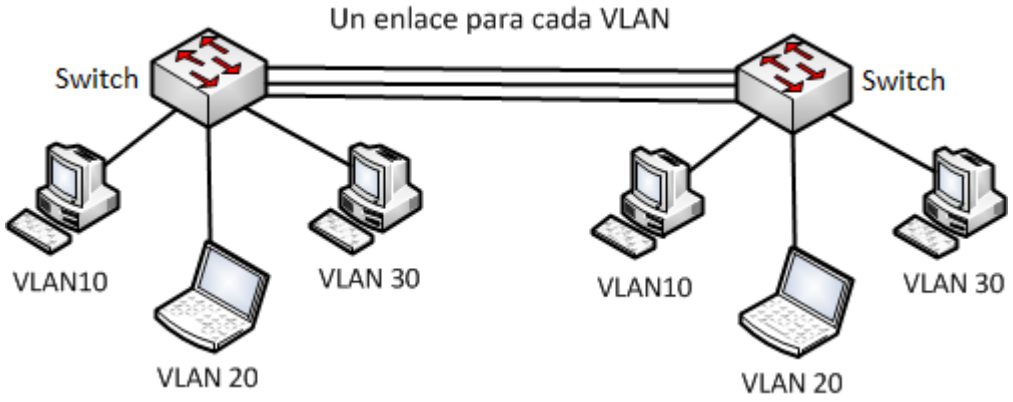

Figura 1.14. Red con interconexión de Switches sin enlace troncal.

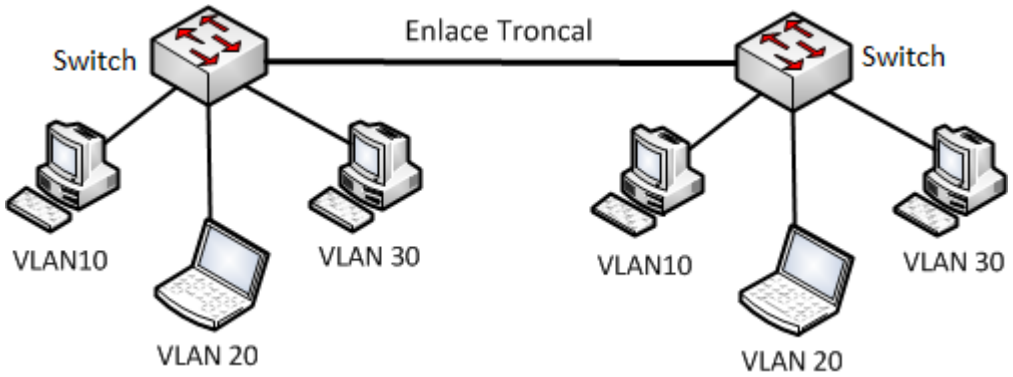

Figura 1.15. Conexión de Switches por medio de enlace troncal.

Los dispositivos que pertenecen a una VLAN determinada en un Switch sólo pueden comunicarse entre ellos mismos. Esto es debido a que una VLAN es un dominio de broadcast independiente de los demás y al generarse mensaje de broadcast o multicast por un equipo, sólo los dispositivos en la misma VLAN los recibirán. Sin embargo, si un dispositivo que se encuentra en una VLAN desea comunicarse con otro en una VLNA diferente, no podrá hacer debido a que se trata de un dominio de broadcast distinto.

Para poder comunicar dispositivos ubicados en diferentes VLAN es necesaria la implementación del ruteo, tarea que un Switch que sólo maneja capa 2 no podrá realizar; no obstante, un Router conectado al Switch a través de un enlace troncal y configurado con la funcionalidad de *Router-on-a-stick* podrá realizar esta tarea sin problema alguno, véase la figura 1.16. La configuración de un Router-on-a-stick hace uso de subinterfaces que representan cada una de las VLAN configuradas en la red. Como ya se había mencionado, la conexión entre el Router y el Switch es a través de un enlace troncal, el tráfico de una VLAN es transportado a través del enlace troncal al enrutador, este verifica que se encuentre en alguna de las redes virtuales a los que se configuró la interfaz que lo recibió y etiqueta la información de la VLAN de destino correspondiente y lo reenvía hacia dicha subred.

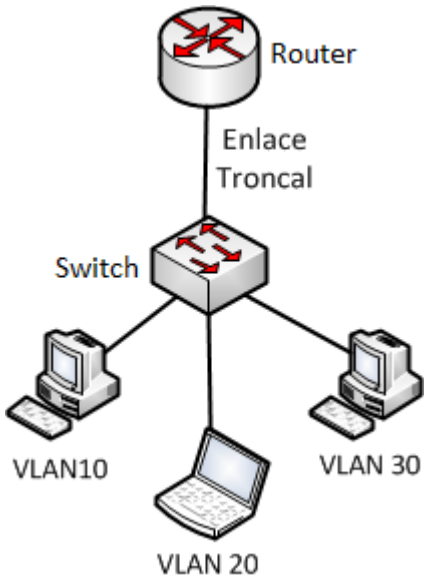

Figura1.16 Router-on-a-stick

Spanning Tree Protocol

Las redes de datos representan un componente fundamental para las pequeñas y grandes organizaciones. Por esa razón, la implementación de mecanismos de redundancia es fundamental para garantizar la continuidad del servicio que se ofrece a los clientes. Tanto en las redes que conectan gran número de Routers y switches, cuando se implementan mecanismos de redundancia existirá una posibilidad alta de generación de ciclos infinitos de tráfico que provoquen que la información no llegue a su destino, genere duplicidad de la misma y por lo tanto la generación de tráfico indeseable en la red de datos.

En una red local que cuenta con varios switches utilizados para conectar a los equipos finales, son conectados físicamente de cierta manera para la conexión de los usuarios, pero también para garantizar que en caso de que uno de los enlaces en la LAN se pierda, otra de las conexiones tome su lugar y continúe el funcionamiento normal de la red.

En la figura 1.17 se muestra una red redundante. Si la PC1 envía una trama de broadcast a la red, este llegará al Switch 2 que actualizará su tabla de direcciones MAC indicando que conoce a la PC1 a través de su puerto FastEthernet 0/10 y enviará la trama a todos sus puertos, incluyendo los enlaces troncales, a excepción del puerto en el que se generó la trama.

Cuando los switches 1 y 3 reciban la trama de broadcast, actualizarán su tabla de direcciones MAC, el Switch 1 indicará que conoce a la PC1 a través de su puerto Fa0/2 y el Switch 1 indicará que conoce a la PC1 por medio de su interfaz Fa0/1. Ambos switches reenviarán la trama a todos sus puertos con excepción del puerto donde la recibieron. De esta manera, Switch 3 recibirá una trama de Switch 1 y viceversas, ambos actualizarán su tabla de direcciones MAC con un puerto incorrecto para la PC1 y volverán a reenviar la trama, provocando que se envíe ambos al Switch 2, mismo que actualizará su tabla de direcciones MAC con la información proveniente de los dos switches. Este proceso se repetirá hasta que alguna de las conexiones que lo provocan se desconecte o uno de los switches que participa en el bucle sea retirado de la red.

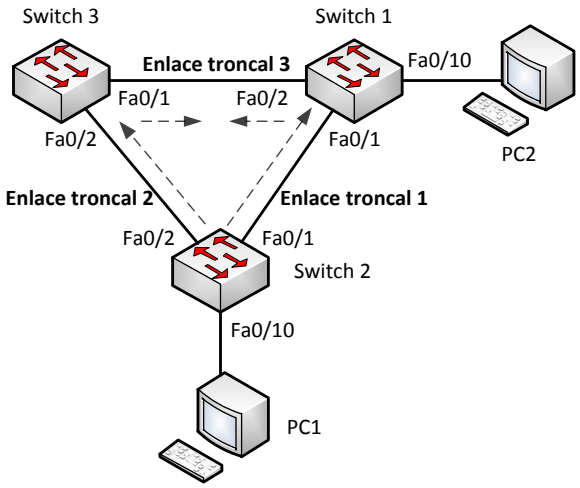

Figura 1.17. Red de switches redundante.

El protocolo de spanning-tree (STP) inició con el estándar **IEEE 802.1D** para evitar loops en las conexiones redundantes entre switches, esto con la finalidad de evitar que las tramas se multipliquen y se transporten entre la red de capa dos sin llegar a su destino final. Esto último provoca sobrecarga del CPU de los dispositivos por la cantidad de datos procesados causado por las tormentas de broadcast y las constantes actualizaciones de tabla de direcciones de MAC con la información inconsistente que esto provoca. Asimismo, la duplicación de tramas genera que el ancho de banda de la red se disminuya haciendo que la comunicación se vuelva imposible. Asimismo, una red con loops provoca duplicidad en las tramas de unicast que se generan en la red.

STP previene la existencia de loops en la red de switches garantizando que sólo exista un camino activo entre cualquier par de segmentos LAN. Esto lo hace gracias a que coloca a las interfaces en los switches en el estado de activo y de bloqueo, en el primero de ellos se envían tramas, mientras que en el último estado no se procesan las tramas, pero si los mensajes de STP llamados BPDU (*Bridge Protocol Data Unit*, Unidad de Datos del Protocolo de Puente).

El BPDU consta de 12 campos, y los más importantes son el IP del puente raíz, el ID del puente emisor (*Bridge ID*, BID), el costo al puente raíz y el valor de los temporizadores. El BID consta de dos campos, la prioridad del puente de 2 bytes y su dirección MAC de 6 bytes. El Switch con la prioridad más baja será el puente raíz; sin embargo, en caso de que todos los switches tengan la misma prioridad, el segundo criterio de selección se basará en

la dirección MAC, el que tenga la dirección más baja será elegido como puente raíz. Este dispositivo tendrá todos sus puertos activos en la red.

En efecto, STP asigna un rol a los puertos de los switches de la red y estos son los que se mencionan a continuación:

- **Puertos raíz:** Son aquellos que se encuentran más cerca al Switch raíz.
- **Puertos designados:** Son puertos que no son raíz pero que pueden enviar tráfico a la red.
- **Puertos no designados:** Puertos que están en estado de bloqueo para evitar loops. No pueden enviar tramas a la red pero si procesan BPDU de STP.

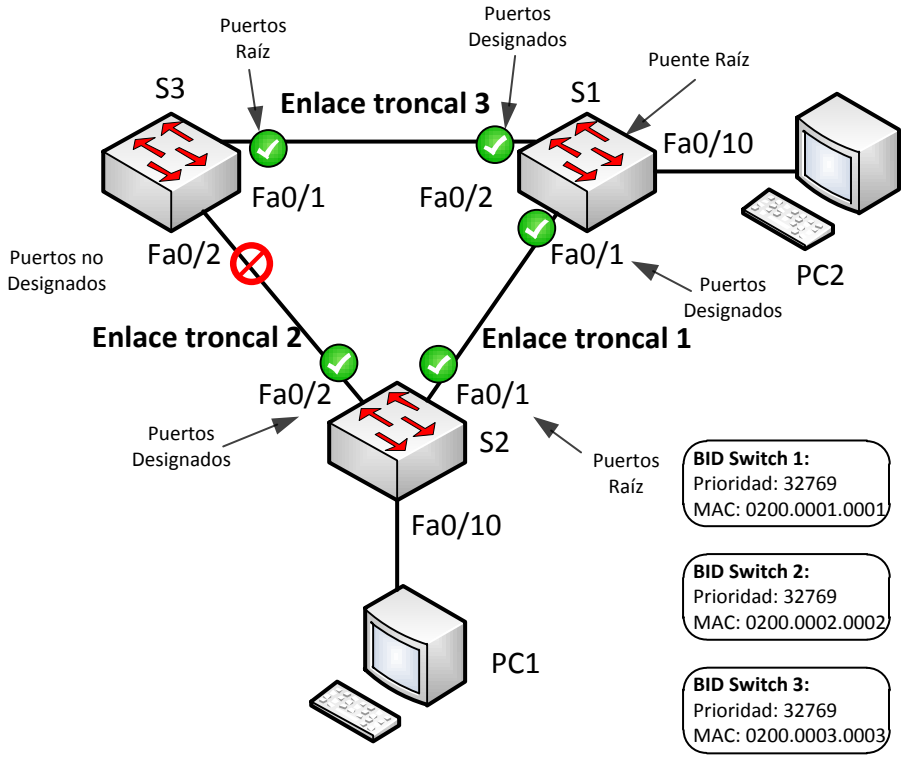

Figura 1.18. Red de switches y STP.

En la figura 1.18 STP ya está en funcionamiento. El Switch 1 es puente raíz para esta red y será tomado como referencia para los cálculos de STP para las rutas redundantes que deben de bloquearse. Para el Switch 1, STP eligió el criterio de la dirección MAC menor para la elección del Switch raíz. De manera predeterminada todos los puertos del Switch raíz son designados.

Asimismo, los switches que no son raíz sólo tienen una interfaz que tiene el rol del "puerto raíz" y es el más cercano al Switch raíz según el costo de la interfaz. Esto lo hace comparando los costos de cada una de sus interfaces. Esto también dependerá del tipo de interfaz, pues según su capacidad será el costo, mientras mayor capacidad, menor el costo. Si se tienen dos puertos con el mismo costo al puente raíz, se elegirá a aquel que tenga el menor ID de puerto, por ejemplo, la interfaz Fa0/1 tiene menor ID que Fa0/2 ya que se toma como ID de puerto al número de interfaz en el Switch, 1 será menor a 2.

En lo que se refiere a los switches que comparten un mismo segmento de LAN, como ocurre con los switches S2 y S3 de la figura anterior, la decisión del puerto designado es a través del BID, el que tenga el BID menor será puerto designado, mientras que el otro puerto será el puerto no designado y se bloqueará.

De esta manera, la PC1 podrá enviar una trama de broadcast a PC2 sin provocar un loop, se tendrá un camino activo a través de la interfaz Fa0/1 de S1. En caso de que ese puerto o su enlace sufran algún daño, el otro camino se activará permitiendo la convergencia de la red.

Si ocurriera un cambio de estado directo del bloqueo a enviar, podría ocasionar un loop en la red. Por tal motivo, STP implementa cinco estados en los puertos y tres temporizadores de BPDU y se explican a continuación:

- **Bloqueo (blocking):** Es un puerto no designado que sólo procesa tramas de BPDU para determinar el ID y la ubicación del Switch raíz, así como las funciones de los puertos que cada dispositivo debe tomar.
- **Escuchar (Listening):** El puerto puede participar en la red activa recibiendo y enviando tramas de BPDU de los switches adyacentes.
- **Aprender (Learning):** El puerto se prepara la para el envío de tramas y empieza a completar su tabla de direcciones MAC.
- **Enviar (Forwarding):** El puerto forma parte de la topología activa y envía y recibe tramas de BPDU.
- **Desabilitado (Disable):** El puerto no participa en spanning-tree y no envía tramas. Es un puerto apagado administrativamente.

Durante un cambio de topología los puertos involucrados sufren la transición entre los estados durante ciertos periodos de tiempo. Para pasar del estado de *bloqueo* al estado de *escuchar* se tiene una antigüedad máxima de 20 segundos. Para pasar del estado de *escuchar* al estado de *aprender*, existe un tiempo de retraso de 15 segundos y para pasar del estado de *aprender* al estado de *envío* existe otro tiempo de retraso de 15 segundos.

Estos temporizadores están calculados para una red con un diámetro de siete switches. El diámetro de una red de switches es la cantidad de dispositivos que atraviesa una trama para llegar a su destino. El valor máximo es de siete, con un diámetro mayor, la red experimentará problemas de convergencia.

En caso de ocurrir un cambio en la topología, el Switch que la detecta enviará una trama BPDU llamada TCN (Notificación de Cambio de Topología) al Switch adyacente a través de su puerto designado, este último dispositivo contestará con una trama TCA (Acuse de Recibo de un Cambio de Topología) y enviará una trama TCN a otro Switch por medio de su puerto designado, así consecutivamente hasta llegar al puente raíz que notificará del cambio de topología a toda la red con una trama TC (Cambio de topología).

Entre las variantes de STP, están las versiones propietarias y las versiones que se especifican como estándares de la industria a través de la IEEE. El protocolo de Rapid Spanning-Tree (RSPT) es una evolución del estándar 802.1D que se incluye en el estándar **IEEE 802.1w**. A diferencia de su antecesor, RSPT ofrece mejoría en los tiempos de convergencia de la red y la agregación de mejoras propietarias, tal es el caso de PortFast (puerto que tendrá ña capacidad de pasar del estado de bloqueo al estado de envío de manera automática) de Cisco ®.

RSPT no utiliza los temporizadores del estándar 802.1D, pero utiliza mensajes de saludos de 2 segundos. De la misma forma, los tipos de puertos y los estados por los que pasa se redefinen. El proceso de recálculo mejora de manera significativa debido a que RSTP converge por enlace y no depende de temporizadores.

En la tabla 1.1, se realiza una comparación de los estados que pasan los puertos entre STP (802.1D) y RSPT (802.1w):

Tabla 1.1. Estados de puerto de RSTP y STP

Estado operativo	Estado de STP (802.1d)	Estado de RSPT (802.1w)	Se envían tramas
Habilitado	Bloqueo (blocking)	Descarte (discarding)	No
Habilitado	Escucha (listening)	Descarte (discarding)	No
Habilitado	Aprendizaje (learning)	Aprendizaje (learning)	No
Habilitado	Envío (forwarding)	Envío (forwarding)	Sí
Deshabilitado	Deshabilitado (disable)	Descarte (disable)	No

RSTP agrega tres roles de puertos más, el puerto alternativo, el puerto de respaldo y el puerto deshabilitado. El puerto alternativo es la interfaz que recibe tramas BPDU menos óptimas que le puerto raíz. El puerto de respaldo se presenta cando se tienen dos puerto en el mismo segmento de la LAN hacia otros dos puertos de otro Switch, uno de ellos será puerto raíz mientras que el otro seré el de respaldo en un estado de descarte. El puerto deshabilitado es aquella interfaz apagada administrativamente, no envía tramas BPDU.

1.1.5 Direccionamiento IP

El Protocolo de Internet IP es fundamental en la capa de Internet del modelo TCP/IP. Este es medular en las comunicaciones que se llevan a cabo hoy en día ya que define un esquema de direccionamiento lógico, especifica el formato de los paquetes de la capa tres, los fragmenta para envío a través de enrutamiento y reensambla cuando los recibe en la comunicación. Asimismo, provee servicios no orientados a conexión.

El Protocolo de Internet utiliza cuatro mecanismos clave para proveer su servicio: Tipo de Servicio, Tiempo de vida, opciones y cabecera de *checksum*. Estos están explicados a detalles en el **RFC 791**.

El Protocolo de Internet versión 4 (IPv4) hace uso de direcciones de red que se componen de 32 bits divididos en cuatro campos de ocho bits. Cada campo de ocho bits toma un valor decimal que va de 0 a 255, o de 00000000 a 11111111 en la forma binaria. Otra versión del Protocolo de Internet es la 6 (IPv6) que cuenta con direcciones de 128 bits de longitud, su desarrollo se dio debido al agotamiento de las direcciones IPv4 que en muy poco tiempo dejará de ser utilizado por dicha causa; sin embargo, este proceso está dándose poco a poco mientras los proveedores de servicios terminan de preparar su infraestructura para el uso de IPv6.

Tabla 1.2a. *Clases de direcciones*

Clase	Rango de direcciones	Máscara de subred	Número de redes y host por red
Clase A	0.0.0.0 a 127.255.255.255	**255**.0.0.0	128 redes, 16777214 host por red
Clase B	128.0.0.0 a 191.255.255.255	**255.255**.0.0	16384 redes, 65534 host por red
Clase C	192.0.0.0 a 223.255.255.255	**255.255.255**.0	2097150 redes, 254 host por red

Tabla 1.2b. *Clases de direcciones*

Clase	Uso	Rango de direcciones
Clase D	Utilizada en grupos multicast en la red.	224.0.0.0 a 239.255.255.255
Clase E	Para investigación y desarrollo. No son asignables para redes IPv4.	240.0.0.0 a 255.255.255.254

Cada dirección IP es utilizada para identificar de manera única a un host en la red. El primer campo de bits determina la clase de la dirección IP. Hay cinco diferentes clases de direccionamiento. Las primeras tres clases son utilizadas para la asignación a dispositivos, mientras que la clase D es utilizada para los grupos de multicast y la clase E es de experimentación.

Las direcciones IP identifican a un host y a una red en particular. Por ejemplo, la dirección 192.168.11.10 es una dirección de clase C, los tres primeros campos de bits representan la red, el último campo es el host.

Dirección IP: 192.168.11.10.

Segmento de la red: 192.168.11.0 (primera dirección IP).

Dirección de broadcast: 192.168.11.255 (última dirección IP).

Por otra parte, es necesario el uso de direcciones públicas (direcciones homologadas) asignadas a equipos que deben de ser alcanzables desde Internet y permiten el acceso a dispositivos que son públicos desde cualquier red; sin embargo, también existen otras direcciones que son utilizadas sobre equipos que no requieren o es limitado su acceso a Internet, estás direcciones son llamadas direcciones privadas (direcciones no homologadas). Esta información se puede encontrar de manera más detallada en el **RFC 1918**.

Los bloques de direcciones no homologadas son:

- De 10.0.0.0 a 10.255.255.255 o 10/8[2]
- De 172.16.0.0 a 172.31.255.255 o 172.16/16
- De 192.168.0.0 a 192.168.255.255 o 192.168.0/16

No obstante, los dispositivos con direcciones no homologadas pueden tener acceso a Internet por medio de algunos servicios, tal es el caso de NAT (Traducción de Direcciones de Red) que permite que un grupo de direcciones privadas sean ruteadas a Internet utilizando una dirección homologada.

Hay diferentes propósitos que cumplen algunas direcciones IP que se mencionan a continuación:

- ***Direcciones de red y broadcast***: La dirección de red es la primera dentro de un dominio de una red e identifica a la misma, la dirección de broadcast es la última dirección y es utilizada para enviar mensajes a todos los dispositivos en la red. Ambas direcciones no son asignables a los dispositivos.

- ***Dirección de ruta predeterminada***: Es utilizada como comodín durante las comunicaciones y el proceso de búsqueda de rutas de un Router. Se representa como 0.0.0.0 y se utiliza cuando no hay rutas a un destino.

- ***Dirección de loopback***: Se utiliza la dirección 127.0.0.1, pero existe un rango de direcciones de loopback que va de 127.0.0.0 a 127.255.255.255. Es utilizada por los dispositivos para enviar tráfico de red hacía ellos mismos. Son utilizadas para pruebas dentro del mismo host.

- ***Direcciones link-local***: Estás direcciones se encuentran en el rango de direcciones IPv4 de 169.254.0.0 a 169.254.255.255. Este tipo de direcciones son utilizados por algunos dispositivos para asignar una dirección a un host que no tiene una configuración IP o no pudo recibir una dirección de un servidor DHCP. Ése tipo de direcciones solo pueden comunicar a la LAN local pero no solicitar servicios de otra red externa.

- ***Direcciones TEST-NET:*** Se encuentran en el rango de direcciones que va de 192.0.2.0 a 192.0.2.255. Tiene fines de enseñanza y documentación de redes. A diferencia de las direcciones experimentales, estás si

[2] La notación utilizada como 10/8 es proporcionada por CIDR.

se permiten en las configuraciones de los dispositivos. Sólo permiten el tráfico dentro de la red local y no hacía Internet.

Al inicio del desarrollo de las comunicaciones a través de la red, se utilizó una clasificación entre las direcciones IP y definían según la clase el tamaño específico de la red y un rango especifico de direcciones. Se asignaba a una organización todo un bloque de determinada clase para la creación de su red. Los protocolos de ruteo que funcionaban en ese momento eran conocidos como *protocolos con clase* tal es el caso de RIP e IGRP.

Naturalmente, el crecimiento de las redes de datos en muy poco tiempo fue bastante rápido y la asignación de direcciones con clase ocasionaba su uso ineficaz y el agotamiento de las direcciones de clase B se estaba dando. No había determinada clase que atendiera los requerimientos específicos de cierta organización. Con ello se desarrolló CIDR (Ruteo entre dominios sin clase) que permite el uso eficaz del espacio de direcciones agregando prefijos a las tablas de ruteo disminuyendo su tamaño ya que es posible especificar rutas que están dirigidas a ciertos segmentos de red con una máscara menor que la que especifica la máscara de la clase. De esta manera los ISP (Proveedores de Internet) asignan espacio de direcciones de manera más eficiente y de tamaños variables según las necesidades de la organización.

Asimismo, el desarrollo de los métodos como la división de subredes o las Máscaras de Subred de Longitud Variable (VLSM) son utilizados para el diseño y planeación del direccionamiento de una red, permitiendo la creación de subredes de diferentes tamaños según los requerimientos propuestos por las organizaciones. Se complementa con CIDR, además de que desata el desarrollo de protocolos de ruteo sin clase, compatibles con CIDR, tales como RIP versión 2, OSPF y EIGRP.

1.1.6 División en de una red en subredes

La división de una red en subredes permite crear múltiples redes lógicas que existen dentro de las redes simples de clase A, B y C, es decir, una subred es un subconjunto de una red de clase. Si no se utilizará esta división, sólo se podría utilizar una red de clase que cumpliera con el requisito de número de direcciones que se necesitan en una organización, que en muchas ocasionas provoca el desperdicio de direccionamiento.

Cada enlace de datos en una red debe tener un identificador de red único, en el que cada miembro del enlace pertenece a la misma red. Si se divide una red mayor (clase A, B o C) en pequeñas subredes, permite crear una red de interconexión de subredes. Cada enlace en esta red tendrá un único identificador de subred. De esta forma, un dispositivo de salida conectará *n* subredes con *n* diferentes direcciones IP.

Para dividir una red en subredes, se extiende la máscara de red de clase, usando los bits de la porción de host para crear un identificador de subred. Por ejemplo, dada la dirección de clase C 204.20.5.0 con su máscara de clase 255.255.255.0 se pueden crear subredes de la siguiente manera:

Tabla 1.3. División de red clase C en 8 subredes de 30 host.

Subred	Máscara decimal	Máscara binaria	Rango de direcciones IP utilizables
204.20.5.0	255.255.255.224	11111111.11111111.11111111.**111**00000	204.20.5.1 a 204.20.5.30
204.20.5.32	255.255.255.224	11111111.11111111.11111111.**111**00000	204.20.5.33 a 204.20.5.62
204.20.5.64	255.255.255.224	11111111.11111111.11111111.**111**00000	204.20.5.65 a 204.20.5.94
204.20.5.96	255.255.255.224	11111111.11111111.11111111.**111**00000	204.20.5.97 a 204.20.5.126
204.20.5.128	255.255.255.224	11111111.11111111.11111111.**111**00000	204.20.5.129 a 204.20.5.158
204.20.5.160	255.255.255.224	11111111.11111111.11111111.**111**00000	204.20.5.161 a 204.20.5.190
204.20.5.192	255.255.255.224	11111111.11111111.11111111.**111**00000	204.20.5.193 a 204.20.5.222
204.20.5.224	255.255.255.224	11111111.11111111.11111111.**111**00000	204.20.5.225 a 204.20.5.254

Como se puede observar en la tabla 1.3, de la máscara de clase se ha extendido tomando tres bits de la porción de host original de la dirección y son usados para hacer subredes. Con esos tres bits es posible crear ocho subredes (**2^3 = 8**). Con los cinco bits restantes de la porción de host, cada subred puede tener 32 direcciones de host (**2^5 = 32**), de los cuales 30 pueden ser asignados a dispositivos, a excepción de las direcciones en las que el identificador de host tiene todos los bits en cero o todos los bits en uno (dirección de red y dirección de broadcast). Por lo tanto, tomando en cuenta lo señalado, se han calcularon las subredes de la tabla anterior.

Hay dos caminos para denotar las máscaras de red. En primer lugar, dado que se están utilizando tres bits más que la máscara de clase, se puede denotar la máscara de red con esos tres bits de más, por ejemplo, de 255.255.255.0 a 255.255.255.224. La segunda forma es utilizando la notación de CIDR, en donde la máscara 255.255.255.224 se puede denotar como /27, ya que hay 27 bits activos en la máscara de subred. Por ejemplo, la red 204.20.5.32/27 denota a la red 204.20.5.32 255.255.255.224.

Mientras se utilicen más bits de la porción de host, más subredes se pueden crear; sin embargo, el número de direcciones por subred disminuye. Por ejemplo, la dirección de clase C 204.20.5.0 con máscara 255.255.255.224 (/27) permite tener ocho subredes, cada una con 32 direccione de red (30 de las cuales pueden ser asignadas a dispositivos). Si se utiliza una máscara de subred 255.255.255.240 (/28) para obtener lo siguiente:

204.20.5.0 11001100.00010100.00000101.00000000
255.255.255.240 11111111.11111111.11111111.**1111**0000

Bits tomados para la subred

De esta manera ahora se tiene cuatro bits para determinar subredes (**2^4 = 16** subredes) y otros cuatro para las direcciones de host (**2^4 = 16** host). En este caso se tiene 16 subredes, cada una con 16 direcciones de host (de las que sólo 14 pueden ser asignadas a dispositivos).

1.1.7 Máscaras de Subred de Longitud Variable (VLSM)

Cuando se divide una red en subredes, todas ellas cuentan con la misma máscara de subred. Esto significa que cada subred tiene el mismo número de direcciones de host disponibles. Esto puede ser utilizado en algunas ocasiones, por otra parte, en la mayoría de los casos, tener la misma máscara de subred en todas las subredes ocasiona también desperdicio de direccionamiento.

Por ejemplo, se tiene la red 204.19.5.0/24 con los siguientes requerimientos en una organización:

- Para la red 1 se necesitan 14 hosts.
- Para la red 2 se necesitan 28 hosts.
- Para la red 3 se necesitan 2 hosts.
- Para la red 4 se necesitan 7 hosts.
- Para la red 5 se necesitan 28 hosts.

La red que requiere mayor número de host es de 28.

Número de nodos = 28	16 < 28 < 32	32 host por subred
Máscara decimal	Número de redes	Número de hosts
255.255.255.224	8	30

Tabla 1.4. Cinco subredes que cumplen con los requerimientos.

Subred	Rango de direcciones IP utilizables
Subred 1: 204.20.5.0/27	204.20.5.0 a 204.20.5.30
Subred 2: 204.20.5.32/27	204.20.5.33 a 204.20.5.62
Subred 3: 204.20.5.64/27	204.20.5.65 a 204.20.5.94
Subred 4: 204.20.5.96/27	204.20.5.97 a 204.20.5.126
Subred 5: 204.20.5.128/27	204.20.5.129 a 204.20.5.158

Al revisar los requerimientos, se puede determinar que se deben crear cinco subredes, en la cual, la subred más grande debe soportar 28 direcciones de host. Esto es posible utilizando una red de clase C utilizando subnetting.

Si se toman tres bits de la porción de host de la dirección de red original, nos permite ocho subredes (2^3) lo que sobrepasa el requerimiento de cinco subredes. Dado lo anterior, quedan cinco bits para la porción de direcciones, 2^5 = 32 (30 usables) cumple con el mayor requerimiento. Por lo tanto, se ha determinado el direccionamiento por medio de subnetting con una red de clase C y la asignación de redes es la siguiente:

Utilizando este método, cada subred no utiliza todas las direcciones de host disponibles, que se traduce en un espacio de direcciones desperdiciado. La figura 1.19 ilustra el espacio de direcciones no utilizado:

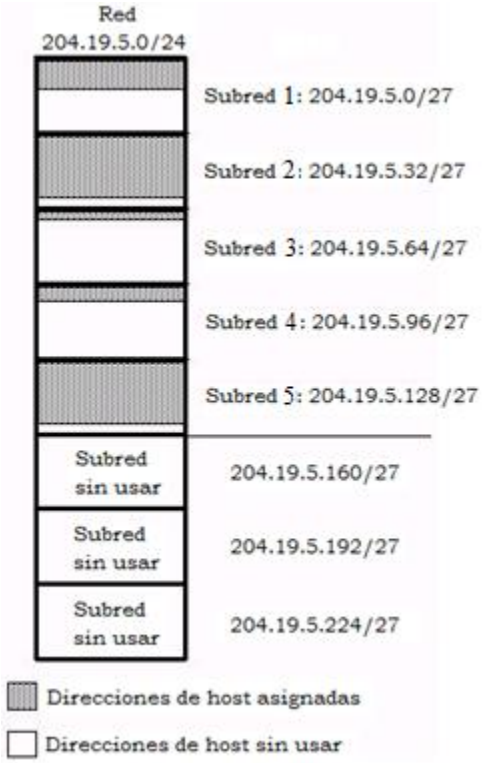

Figura 1.19. Espacio de direcciones del cálculo de subredes.

Se puede observar que cada una de las subredes tiene un gran espacio de direcciones de host sin utilizar. Es posible que se tratase de un diseño deliberado que tome en cuenta un crecimiento futuro, pero en la mayoría de los casos se desperdicia el espacio de direcciones debido a que se trata de la misma máscara de subred para todas las subredes.

VLSM permite el uso de máscaras de subred diferentes, utilizando de manera eficiente el espacio de direcciones.

Con la misma red y requerimientos, se procede a ordenar la lista de requerimientos del mayor número de host al menor de la siguiente manera:

- Para la red 1 se necesitan 14 hosts.

Número de nodos = 14	8 < 14 < 16	16 host por subred
Máscara decimal	Número de redes	Número de hosts
255.255.255.240	16	14

- Para la red 2 se necesitan 28 hosts.

Número de nodos = 28	16 < 28 < 32	32 host por subred
Máscara decimal	Número de redes	Número de hosts
255.255.255.224	8	30

- Para la red 3 se necesitan 2 hosts.

Número de nodos = 2	2 < 2 < 4	4 host por subred
Máscara decimal	Número de redes	Número de hosts
255.255.255.252	64	2

- Para la red 4 se necesitan 7 hosts.

Número de nodos = 7	8 < 7 < 16	16 host por subred
Máscara decimal	Número de redes	Número de hosts
255.255.255.240	16	14

- Para la red 5 se necesitan 28 hosts.

Número de nodos = 28	16 < 28 < 32	32 host por subred
Máscara decimal	Número de redes	Número de hosts
255.255.255.224	8	30

Tabla 1.5. Subredes haciendo uso de VLSM.

Subred	Rango de direcciones IP utilizables
Subred B: 204.20.5.0/27	204.20.5.1 a 204.20.5.30
Subred E: 204.20.5.32/27	204.20.5.33 a 204.20.5.62
Subred A: 204.20.5.64/28	204.20.5.65 a 204.20.5.78
Subred D: 204.20.5.80/28	204.20.5.81 a 204.20.5.94
Subred C: 204.20.5.96/30	204.20.5.97 a 204.20.5.98

Para el cálculo de las subredes, se empezará a dividir la red desde la subred más grande. Una máscara /29 (255.255.255.248) permite 6 direcciones de host usables, la red D requiere de 7 host, por lo que se utilizará la máscara /28 que permite 14 host utilizables.

Las subredes que resultaron de este cálculo se pueden observar en la tabla 1.5.

El espacio de direcciones puede quedar representado gráficamente por medio de la figura 1.20:

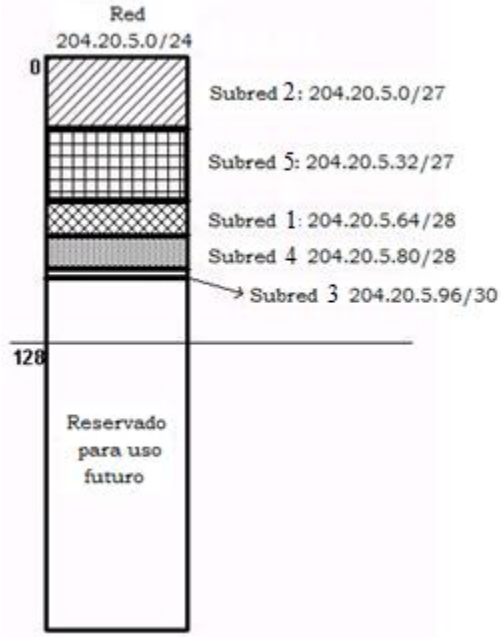

Figura 1.20. Espacio de direcciones con VLSM

Por medio de VLSM el uso del espacio de direccionamiento es sólo el requerido, dejando un espacio reservado para crecimiento de la red en el futuro.

1.1.8 Tipos de ruteo

El Router tiene como tareas fundamentales encontrar el mejor camino y el reenvío de paquetes. El ruteo es la acción en la que ese dispositivo transmite información de una red origen a otra de destino. Asimismo, obtiene información de redes remotas de manera dinámica utilizando protocolos de ruteo, o de manera manual, utilizando rutas estáticas. Debido a esto, se puede determinar que hay dos tipos de ruteo, el estático y el dinámico.

Muchos de los procedimientos utilizados para enrutar paquetes a través de la red basan su funcionamiento en diferentes métricas y algoritmos que no son compatibles entre sí. En una red donde se utilizan diversos protocolos de enrutamiento, el intercambio de información de ruteo y la capacidad de elegir la mejor ruta es crítico.

Para poder implementar varias soluciones en una misma red es utilizado el concepto de *Distancia Administrativa* que es una característica utilizada por los Routers para la elección de la mejor ruta cuando se tienen dos o más rutas a un mismo destino dado por diferentes protocolos de ruteo. La distancia administrativa define la confiabilidad de un protocolo de ruteo. Cada protocolo de ruteo es ordenado por prioridad del más al menos fiable por medio de la distancia administrativa.

Los diferentes tipos de ruteo se explican en los siguientes puntos.

1.1.8.1 Ruteo estático

Este tipo de ruteo se utiliza cuando se han configurado rutas estáticas en el dispositivo. Las rutas estáticas se utilizan cuando se reenvían paquetes de una red a otra a través de una conexión única. Estas son fáciles de configurar y se hace de manera manual; sin embargo, esta acción sólo es viable cuando la red es pequeña ya que se convierte en una operación complicada conforme la red crece.

En este tipo de ruteo no existe el intercambio de mensajes acerca de la topología de la red entre los equipos. Las rutas describen caminos a redes conocidas y son introducidas al dispositivo por el administrador de la red. Una red entera puede estar configurada usando rutas estáticas, pero no es una configuración tolerante a fallas.

Las rutas estáticas que se configuran en el enrutador utilizan la dirección IP del equipo siguiente (Router del siguiente salto) en el enlace físico o el nombre de la interfaz de salida dentro de la sentencia. Cuando se utiliza la dirección IP del siguiente salto, el equipo debe resolver la dirección con la interfaz de salida. El uso de la interfaz de salida es efectivo cuando se utilizan enlaces punto a punto, ya que no existe dirección IP que se tenga que resolver a una interfaz volviéndose un procedimiento más rápido.

Las rutas estáticas tienen una distancia administrativa de "1", tanto las rutas configuradas con una dirección IP del siguiente salto o una interfaz de salida.

La ruta estática con dirección IP del siguiente salto se guarda en tabla de ruteo si la dirección puede resolverse a una interfaz de salida. Si la ruta estática se encuentra configurada con una dirección IP del siguiente salto o una interfaz de salida, esta va a ser incluida en la tabla de ruteo si la interfaz de salida se encuentra ya en la tabla.

El ruteo estático es utilizado en contextos donde los protocolos de ruteo no son posibles de implementar, por ejemplo, en soluciones que proporcionen seguridad, por ejemplo, cuando es utilizado un firewall[3]en el que se permita cierto tráfico de datos a redes que no están directamente conectadas, se tiene que definir una ruta estática o una ruta predeterminada a interfaces permitidas o a redes de confianza.

La sintaxis para la configuración de una ruta estática en cualquier dispositivo es la siguiente:

Comado agregar ruta *<Identificador_de_red_destino> <máscara_de_subred> {<Interfaz_de_salida> y/o <Dirección_IP_Siguiente_salto>}{métrica}*

El comando para agregar una ruta estática va a depender del sistema operativo del dispositivo que esté ejecutando el rol de Router en la red, puede ser un equipo de red comercial de red o incluso una PC sobre Unix que ejecute la función de reenvío de paquetes. Los parámetros comunes en una ruta estática son: el identificador de la red a la que se apunta la ruta estática, la máscara de subred y la interfaz por la que el Router va a eviar el tráfico hacia esa red específica. Algunos equipos aceptan ciertos tipos de definiciones para una ruta estática, estos se han denotado entre llaves en la sintaxis presentada. La *interfaz de salida* es la interfaz por la que el equipo enviará los paquetes con destino a la red especificada en la ruta estática, este parámetro puede ser reemplazado o configurado en conjunto con la *dirección IP del siguiente salto* que es la dirección IP de la interfaz del equipo que está en el extremo de la conexión. Es posible determinar una métrica en la ruta estática, este parámetro es utilizado cuando se tienen diversas rutas a una misma red, pero sólo se desea utilizar una y dejar las otras de respaldo, si o se utiliza el parámetro este valor es "1" de manera predeterminada, mientras sea menor el valor, es la ruta que se va elegir para ser utilizada.

[3]Se tratará acerca del firewall posteriormente.

1.1.8.2 Ruteo por defecto

Es posible que un Router que tenga configurado muchas rutas no se hayan especificado alguna de ellas a una red conocida; sin embargo, es posible configurar una ruta estática que sea general y represente todas las redes, y esa es la *ruta por defecto (default route)*. Esta ruta tiene incluidas a todas las redes. Si el Router durante la búsqueda de una ruta a una red en su tabla de ruteo y no encuentra alguna entrada que coincida, pero se tiene configurada la ruta por defecto (también llamada ruta predeterminada), se enviarán los datos a la interfaz que esta indique.

Es común que la configuración de la ruta por defecto se realice en el equipo que está conectado al enlace con el proveedor de servicios de Internet, ya que es imposible tener configurado en ese dispositivo todas las rutas de Internet ya que estás son demasiadas y es imposible para un dispositivo de acceso de un cliente soportar el procesamiento de una cantidad enorme de información de ruteo.

La configuración de la ruta predeterminada es la misma que se utiliza para la configuración de una ruta estática normal; sin embargo, el identificador de red es 0.0.0.0 y la máscara de subred es 0.0.0.0. Estos dos valores indican al dispositivo que se conocen al rango de redes que inicien desde 0.0.0.0 hasta 255.255.255.255, pues los ceros en la máscara de subred indican los bits que pueden cambiar por campo de 8 bits, la ruta predeterminada indica todos los bits de la dirección.

Todo dispositivo tiene una ruta por defecto. Usualmente se utiliza la dirección del dispositivo del siguiente salto, es decir, la dirección IP de la interfaz del equipo que está conectado al otro extremo de la conexión que da salida al equipo.

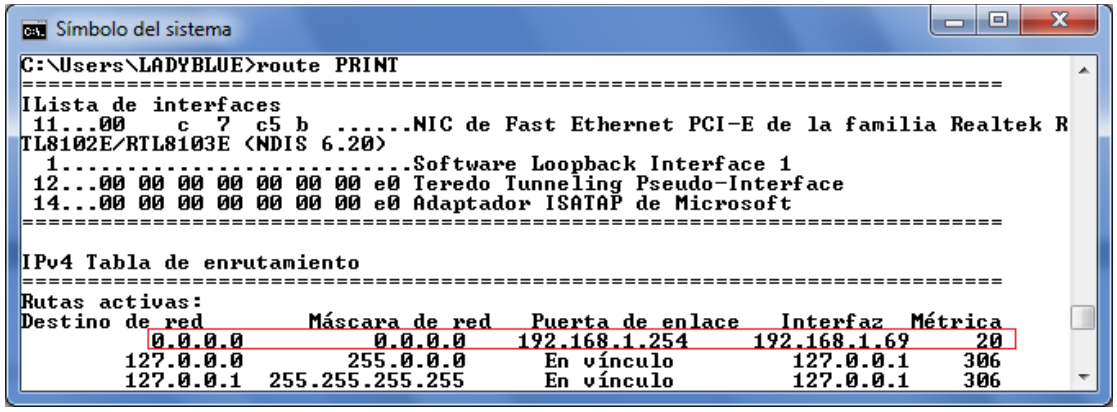

Figura 1.21. Tabla de ruteo de un equipo de cómputo personal sobre Windows.

En la figura 1.21 se presenta el despliegue de una tabla de ruteo de un equipo de cómputo personal sobre el sistema operativo Windows. Cada equipo tiene un parámetro configurado llamado *Dirección de puerta de enlace predeterminada* que se trata de la dirección IP del dispositivo que le da salida a Internet a la PC. Cuando se despliega la tabla de ruteo, se puede observar que se trata de una ruta estática por defecto ya que la red de destino y su máscara de subred es 0.0.0.0 y 0.0.0.0, la dirección de puerta de enlace es la dirección del siguiente salto y el dato que se despliega como “Interfaz” indica que los paquetes que se manden a través de la ruta por defecto serán enviados a la interfaz de salida con la dirección IP que se muestra en la imagen 1.22.

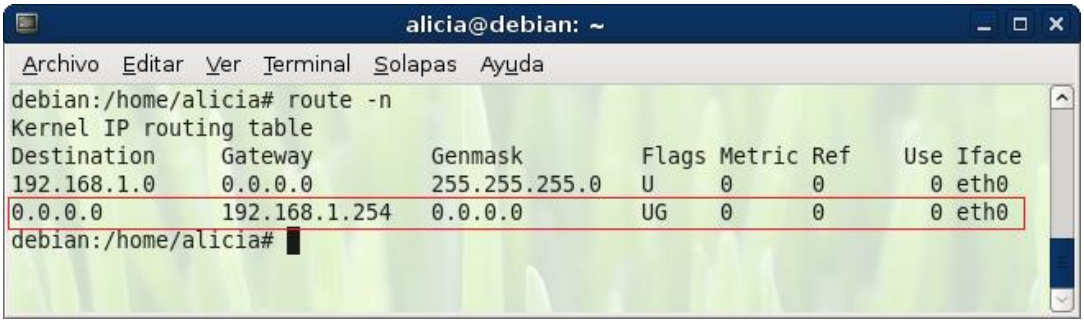

Figura 1.22. Tabla de ruteo de un equipo de cómputo personal sobre Linux.

La mayoría de los dispositivos cuentan con una ruta por defecto ya que permite que la tabla de ruteo sea más pequeña. En los equipos personales, la tabla de ruteo puede ser de una sola entrada de información, para poder llegar desde ese dispositivo a cualquier sitio de Internet sólo es necesario conocer esa ruta, el proveedor de servicios es el encargado de hacer el resto para que se permita la comunicación.

1.1.8.3 Ruteo dinámico

Este tipo de enrutamiento hace uso de protocolos dinámicos los cuales son configurados en los Routers para obtener información sobre redes remotas de provistas por otros dispositivos de manera automática.

La información que se comparte entre dispositivos matutinos es característica del protocolo de ruteo que se haya implementado entre un grupo de Routers.

Los protocolos de ruteo se clasifican como: con clase y sin clase, vector distancia o estado-enlace, Gateway interior o Gateway exterior.

Los Routers que utilizan protocolos *con clase* envían información acerca de sus redes sin enviar la máscara de subred. El tipo de máscara es determinada por el Router que recibe la información por medio del análisis de la dirección de la red analizando su primer grupo de bits para determinar su clase y a su vez la máscara de subred que le corresponde. Los protocolos *sin clase* envían en la información de ruteo la máscara de subred, ya que soportan VLSM y CIDR, y son los más utilizados en las redes actuales.

Los protocolos *vector distancia* proporcionan la información de la métrica a utilizas por medio de magnitudes (por ejemplo, número de saltos a una ruta) y una dirección. Los protocolos *estado-enlace* hacen referencia a los enlaces (conexiones entre Routers) que incluyen la dirección IP de la interfaz y su máscara de subred, tipo de red, costo y cualquier dirección a un dispositivo vecino.

Los protocolos de *Gateway interior* son utilizados para el ruteo dentro de sistemas autónomos, mientras que los protocolos de *Gateway exterior* redireccionan sistemas autónomos.

Los protocolos de ruteo no sólo descubren redes remotas sino que también tienen procedimientos para mantener la información actualizada y precisa. Cuando ocurre un cambio en la topología de la red, es tarea del protocolo de ruteo informar a los demás Routers sobre dicho cambio.

Cuando ocurre un cambio en la topología de red, algunos protocolos de ruteo propagan la información más rápido que otros. El proceso de mantener toda la tabla de ruteo con información precisa y actualizada se llama *convergencia*.

Los protocolos de ruteo usan métricas para determinar el mejor camino o ruta más corta. Cada protocolo de ruteo utiliza métricas distintas. Las métricas menores indican un mejor camino. Para lograr una mejor conexión son mejor tres saltos que once.

Tabla 1.6. Distancias administrativas

Fuente de ruta	Valor de Distancia Administrativa
Interfaz conectada	0
Ruta estática	1
Ruta sumarizada EIGRP	5
EIGRP interno	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externo	170

Cuando los Routers obtienen información de ruteo por medio de rutas estáticas y protocolos de ruteo, así como información a una misma red por medio de diferentes protocolos de ruteo, la elección de la mejor ruta la determinará la distancia administrativa. Cada protocolo de ruteo utiliza un valor de distancia administrativa único. Una red conectada directamente es preferida, seguida de las rutas estáticas y luego los protocolos de ruteo.

1.2 Seguridad Informática

La información es el activo más importante para las organizaciones y las personas, esta debe mantener tres características valiosas: ser confidencial, ser integra (sin cambio alguno) y disponible en cualquier momento al usuario. En los puntos siguientes se tratarán los conceptos de la seguridad informática, mismos que se aplicarán a este trabajo.

1.2.1 Definición de seguridad informática

La información son un conjunto de datos que tienen cierto significado para alguien. Esta debe estar resguardada y disponible sólo para personas autorizadas que pueden tener los privilegios de leerla, no de modificarla. Es evidente que proteger estos datos se vuelve fundamental, por tal motivo aparece el concepto de *seguridad informática* tratándose del conjunto de protecciones que permiten resguardar la información. Hay que tener en cuenta que la información se puede presentar de dos formas: impresa o digital, volviéndose la última la más común actualmente, debido al crecimiento tecnológico. Ahora la mayoría de la información se presenta como documentos digitales almacenados en discos duros y viajan a través de la red cuando se transmite la información.

Por consiguiente, la *seguridad informática* son un conjunto de protecciones que permiten salvaguardar los datos digitales e informáticos. Por otra parte, la transmisión de la información también tiene que ser resguardada, por lo que también se establece la *seguridad en la red*.

La seguridad informática se compone de reglas, normas, procedimientos, técnicas y métodos destinados para conseguir un sistema seguro y confiable.

Para poder diseñar y después implementar un esquema de seguridad que nos permita mantener segura nuestra información, es necesario seguir cierta metodología que nos ayudará a identificar que proteger y de qué. Para eso,

preguntas como las siguientes ayudan a los administradores de red y de sistemas de información desarrollar un proyecto de seguridad: ¿Qué se quiere proteger? ¿Qué tan dispuesto se está de perderlo? ¿Si se pierde, cuáles son las consecuencias? ¿Si en este momento no se cuenta con el bien haría falta? Las preguntas anteriores detectan el bien y le asignan un valor, ¿De qué se quiere proteger? Detecta que podría afectar a los bienes, ¿Cómo se va a proteger? Permite la identificación y creación de las acciones y herramientas que se usarán para mantener a salvo los bienes.

¿De qué se debe proteger la información? Se dice que se ha producido un ataque accidental o deliberado contra el sistema cuando se ha materializado una amenaza.

En función del impacto causado a los activos atacados, los ataques se clasifican en:

- ***Activos:*** Si modifican, dañan, suprimen o agregan información, o bien bloquean o saturan los canales de comunicación.
- ***Pasivos:*** Solamente acceden sin autorización a los datos contenidos en el sistema. Son los más difíciles de detectar.

Un ataque puede ser directo o indirecto, si se produce desde el atacante al elemento "víctima" directamente, o a partir de recursos o personas intermediarias.

El ataque cometido por parte de un hacker que utiliza computadoras intermediarias para ocultar la propia identidad (IP) hasta llegar a su objetivo es un ataque indirecto.

Los protocolos utilizados en la comunicación en su gran mayoría carecen de seguridad, y a medida que evolucionan las comunicaciones y la variedad de dispositivos, aumentan la diversidad de los ataques.

Asimismo, los tipos de atacantes se pueden clasificar en dos tipos: *internos (insiders)* o *externos (outsiders)*. Los atacantes internos son ocasionados por personal que pertenece a la organización, usualmente causan daños sin intención, debido a errores y descuidos; sin embargo, no se descarta que los ataques de este tipo sean intencionales. Los atacantes externos no pertenecen a la organización, y buscan principalmente causar un daño a la organización deliberadamente, así como la complejidad de los ataques es alta, ya que se debieron haber roto varias reglas para llegar a su objetivo.

Es importante tener controles de seguridad, que son procedimientos que se llevan a cabo para salvaguardar nuestro sistema y se pueden llevar a cabo en tres controles fundamentales:

Físico: Estos controles implementan seguridad a las instalaciones de nuestro sistema, es decir, a los racks, servidores y dispositivos de interconexión, de daños a su funcionamiento e impedir el acceso no permitido a las instalaciones. Entre las herramientas utilizadas se tienen: Candados, cámaras de circuito cerrado, guardias de seguridad, identificadores biométricos, puertas de acero con seguros especiales.

Técnico: Estos controles se implementan en los sistemas informáticos, es decir, a los sistemas operativos ya sea de usuario, servidores y de interconexión a través de la red. Entre ellas se encuentran: criptografía, certificados, huellas digitales, listas de control de acceso (ACL), protocolos simples de cifrado y descifrado, autenticación, herramientas de gestión y monitorización, firewalls, entre muchas otras.

Administrativo: Estos controles definen como trabajaran las personas en el sistema informático ya sea local o remoto a través de la red, determinando como es que se va a acceder y cuáles serán los privilegios según la clasificación de usuarios. Entre los controles de este tipo se tienen: creación de políticas de seguridad, capacitación y educación del personal, herramientas de gestión de claves y de monitorización.

1.2.1.1 Servicios de seguridad

Los *servicios de seguridad* ayudan a mejorar la protección de un sistema de información, evitando los ataques mediante la utilización de uno o varios mecanismos de seguridad con el objetivo de resguardar la información. Estos servicios son los siguientes:

Servicio de autenticación

Este servicio asegura que las entidades que se comunican son quién reclaman ser; corrobora la identificación correcta del origen del mensaje.

El servicio de autenticación define dos servicios específicos:

- Autenticación del origen de los datos: Se aplica a comunicaciones no orientadas a conexión donde las unidades de datos son independientes. Garantiza que el origen de cada unidad de datos corresponde con la indicada en su cabecera. Puede ofrecerse en aplicaciones como el correo electrónico, donde no hay una comunicación previa entre entidades finales.
- Autenticación de entidades pares: Se aplica a comunicaciones orientadas a conexión. Asegura la identidad de las dos entidades que se comunican, es decir, se asegura que cada una es quién dice ser. Asimismo en la fase de transferencia debe garantizar que un intruso no pueda suplantar a cualquiera de las dos entidades legítimas que se comunican a efectos de transmisiones o recepciones no autorizadas.

Servicio de control de acceso

Evita el uso no autorizado de los recursos. Controla quien puede tener acceso a un recurso, bajo qué condiciones puede tener lugar el acceso y que se le permite hacer a aquel que accede a un recurso.

Servicio confidencialidad de datos

Asegura que la información o no va a ser revelada ni va a estar disponible a individuos no autorizados, entidades o procesos.

Se han descrito cuatro versiones de este servicio:

- Confidencialidad orientada a conexión: Consiste en la protección de todos los datos de usuario en una comunicación orientada a conexión.
- Confidencialidad no orientada a conexión: Consiste en la protección de todos los datos de usuario contenidos en una sola unidad de datos del servicio (UDS) en una comunicación no orientada a conexión.
- Confidencialidad selectiva: Consiste en la protección de campos específicos de todas las unidades de datos de usuario de una comunicación orientada a conexión o de una sola unidad de datos del servicio (UDS) en una comunicación no orientada a conexión.
- Confidencialidad aplicada al análisis del tráfico: Brinda protección a los datos frente a un análisis del tráfico originado por una comunicación entre entidades pares.

Servicio integridad de datos

Asegura que los datos que son recibidos sean exactamente a como han sido enviados por una entidad autorizada, es decir sin duplicaciones, retransmisiones, modificaciones o inserciones. Cuando se detecta una violación en la integridad de los datos, el servicio de integridad puede avisar de que se ha producido este hecho o utilizar mecanismos para la recuperación de la perdida de integridad de los datos.

Se han definido cinco modalidades de este servicio:

- Integridad orientada a conexión con mecanismos de recuperación: Proporciona la integridad de los datos de usuario en una comunicación orientada a conexión asimismo detecta cualquier modificación, inserción, borrado o retransmisión de cualquier unidad de datos haciendo uso de mecanismos de recuperación de la integridad si fuera necesario.
- Integridad orientada a conexión sin mecanismos de recuperación: Proporciona integridad de los daros durante una conexión, detecta las violaciones en la integridad de los datos pero no se articulan mecanismos de recuperación de la integridad.
- Integridad orientada a conexión sobre campos selectivos: Asegura la integridad de campos específicos dentro de las unidades de datos de usuario en una comunicación orientada a una conexión y determina si los campos seleccionados han sido modificados, insertados, borrados o retransmitidos.
- Integridad no orientada a conexión: Asegura la integridad de una sola unidad de datos del servicio (UDS) en comunicaciones no orientadas a conexión.
- Integridad no orientada a conexión sobre campos selectivos: Asegura la integridad de campos específicos dentro de una sola unidad de datos del servicio (UDS) en comunicaciones no orientadas a conexión. Determina si los campos seleccionados han sido modificados.

Servicio no repudio

Evita que las entidades pares que se comunican puedan denegar el haber participado en parte o en toda la comunicación. Se han definido dos modalidades del servicio:

- No repudio con prueba de origen: Proporciona los mecanismos necesarios al destinatario para asegurar que el mensaje fue enviado por la entidad especificada.
- No repudio con prueba de entrega: Proporciona los mecanismos necesarios para asegurar que el mensaje fue recibido por la entidad especificada.

1.2.1.2 Mecanismos de seguridad

Los mecanismos de seguridad ya son las herramientas que se utilizan para implementar cada uno de los servicios de seguridad. Se podrían utilizar más de un mecanismo de seguridad para cubrir uno de los servicios de seguridad.

Existen dos tipos fundamentales, los específicos y los generalizados:

1. Mecanismos de seguridad específicos

- *Mecanismo de cifrado*

El cifrado es el mecanismo utilizado para presentar de manera inteligible la información de tal manera que no pueda ser entendida por terceras personas, y su uso es muy utilizado en las comunicaciones.

Hay dos funciones principales, el cifrado y el descifrado y es utilizado para brindar los servicios de seguridad de integridad, autenticación y confidencialidad.

Su uso es muy variado, y su principal función se encuentra en las comunicaciones, y se ha ido desarrollando protocolos y estándares, tales como AES (Advanced Encryption Standard), y la gran aportación de Claude Shannon y su publicación acerca de la seguridad en las comunicaciones y el cifrado de llaves asimétricas.

- *Mecanismo de firma digital*

La firma digital es un mecanismo que ofrece las propiedades para la verificación del autor de la información, de esta manera sirve como autenticación de los contenidos

- *Mecanismos de control de acceso*

Este mecanismo permite asegurar que sólo usuarios autorizados tenga acceso a un sistema de información, y se puede limitar al usuario a entrar al sistema y brindar ciertos privilegios para operar con los recursos brindados en él.

- *Mecanismo de integridad en los datos*

Este mecanismo determina si la información que fue transmitida durante un proceso de comunicación ha llegado sin cambios. Este mecanismo está ligado muy ampliamente al protocolo de transmisión de datos utilizados. Para implementar el mecanismo de integridad durante la transmisión de un conjunto de datos se puede utilizar el protocolo TCP (Transmission Control Protocol) que en su PDU implementa un campo llamado cheksum, así como números de secuencia, que permiten que la información llegue sin modificación y en orden a su destino.

- *Mecanismos de Intercambio de Autenticación*

Los mecanismos de este tipo verifican después de una comunicación, que los datos recibidos sean auténticos y provengan del usuario del que dicen ser.

- *Mecanismos de Relleno de Tráfico*

Este mecanismo es utilizado para la generación de paquetes cifrados que usualmente carece de texto claro sino que es información aleatoria y ocasione confusión a los atacantes que se dedican al análisis de tráfico estudiando las cabeceras de los paquetes de información transmitidos. El receptor debe ser capaz de determinar el flujo correcto y el inválido debido que previo a la comunicación se estableció una secuencia de bits que le permitirá identificarla.

- *Mecanismo de control de encaminamiento*

Permite identificar las rutas donde se ha presentado ataques a la información en determinadas rutas, y así elegir otras alternativas.

- *Mecanismo de certificación*

Este mecanismo permite que el emisor demuestre quien es. Usualmente se usan en la transmisión de documentos, programas, envío de correos. Los certificados son seguros si una Autoridad Certificadora (Certification Authority, CA). Los certificados implementan mecanismos criptográficos que implementan autenticación.

2. Mecanismos de seguridad generalizados

- *Mecanismo de funcionalidad de confianza*

La funcionalidad digna de confianza provee protección de asociaciones encima de la papa en la cual es aplicada. Esto permita determinar el grado de confianza de determinado servicio, asociación o persona.

- *Mecanismo de etiqueta de seguridad*

Se trata de números que permiten graduar la sensibilidad de determinados datos clasificando la información por niveles de seguridad: secreta, confidencial, no clasificada, etc.

- *Mecanismo de detección de eventos*

Un mecanismo de gestión de eventos permite identificar acciones que no están permitidas en el sistema y actúa de manera inmediata por medio de notificaciones locales y remotas, finalización de la sesión o acciones de recuperación.

- *Mecanismo de auditoría de seguridad*

Se hace por medio de un archivo o una auditoría que permite revisar y probar el funcionamiento de los servicios y los mecanismos utilizados y verificar si se adecuan a las políticas de seguridad.

- *Mecanismo de recuperación de seguridad*

Está muy ligado al mecanismo de detección de eventos y se lleva a cabo acciones siguiendo un conjunto de reglas. Los procedimientos que se llevan a cabo pueden ser inmediatos o temporales.

1.2.1.3 Amenazas

Las amenazas son todos aquellos factores (humanos, físicos, tecnológicos o eventos) que pueden tacar el sistema si tienen oportunidad, dependiendo del grado de vulnerabilidad del punto atacado. Las amenazas pueden o no manifestarse. Hay diferentes tipos de amenazas que podrían afectar a un sistema de información, desde las físicas (fallas en las instalaciones eléctricas, fallas de hardware por ejemplo), el uso de software malintencionado como virus e incluso el robo y alteración de la información.

Las amenazas se pueden clasificar dependiendo del daño que causen a la información y al sistema, particularmente se presentarán tipos de amenazas que se presentan sobre la información, particularmente durante las comunicaciones:

Intercepción

La amenaza se encuentra en medio de la comunicación entre dos nodos que comparten información y se comunican sin la menor idea que otro. No interrumpe la comunicación ni modifica la información, pero tienen acceso a los datos confidenciales.

Interrupción o destrucción

La información se envía de un nodo a otro en la comunicación; sin embargo, la información no llega al segundo negándole la disponibilidad de la información. Otra forma en la que se presenta este tipo de amenaza es destruyendo los medios de almacenamiento como discos duros, bloqueando los acceso a la información, así como la carga de los medios de comunicación para evitar el acceso a los sistemas.

Modificación

Durante la comunicación entre dos nodos, la amenaza se encuentra informado de la comunicación e intercepta la información modificándola y colocándola nuevamente en el medio para que llegue a su destino; sin embargo, los datos no son los mismos habiendo sufrido un ataque a la integridad de la información.

Suplantación

Durante la comunicación entre dos nodos, el receptor recibe información de un emisor que no es el indicado, debido a que la amenaza se ha hecho pasar por él. La información recibida no es la correcta debido a que no proviene del emisor original.

También se puede realizar una clasificación de las amenazas según el origen de las mismas:

Intencionadas

Usuarios autorizados del acceso a la información hacen abuso de su autoridad así como también personas no autorizadas que logran tener acceso de forma indebida al sistema. Ya habiéndose realizado la intrusión, pueden

ejecutar códigos maliciosos que afecten a la información y realizar el robo y modificación de la información. Estas amenazas pueden tener su origen en el exterior de la organización o puede ser ocasionado por personal de la misma.

No intencionadas

Usualmente provienen por descuidos o errores en los propios sistemas como en el hardware o sistema operativo. Asimismo, se pueden generar por el trabajo inadecuado de personal mal capacitado que no manipula correctamente la información y las herramientas causándoles daños.

Para poder identificar las amenazas que podrían afectar a un sistema de información es recomendable pensar e imaginar cualquier suceso que podría sucederle a los activos que salvaguardan la información.

1.2.1.4 Vulnerabilidades

Las vulnerabilidades son puntos débiles que posee el sistema de información. Estás son explotadas por las amenazas para que se presente un ataque. Cada activo en una organización tiene sus propias vulnerabilidades, no son las mismas, por lo que es importante hacer la identificación de las vulnerabilidades para cada activo.

Es más, es posible que haya ciertas relaciones entre amenazas y vulnerabilidades, como se indica a continuación:

- Varias amenazas explotan varias vulnerabilidades.
- Una amenaza explota varias vulnerabilidades.
- Una amenaza explota una vulnerabilidad.
- Varias amenazas explotan una vulnerabilidad.

Es importante realizar un análisis de riesgos para la identificación de los posibles ataques que podrían suceder, cuales son las vulnerabilidades del sistema y valorar las amenazas. Un riesgo es la posibilidad que una amenaza aproveche una vulnerabilidad.

Analizar los riesgos de un sistema de información implica un proceso de análisis de activos, sus vulnerabilidades, las amenazas que existen, medidas de seguridad que se tienen implementadas al momento, determinación del impacto que ocasionaría cierto ataque sobre alguno de los activos, identificación de los objetivos de seguridad de la organización y de las medidas que se tomarán para poder cubrir tales objetivos.

1.2.2 Políticas de seguridad informática

Una política de seguridad es un conjunto de pautas que establece la organización para proteger los recursos de red de la misma ante ataques que provengan del exterior o generadas internamente. Para poder generar una política de seguridad es importante conocer las acciones que se llevan a cabo en la red para que los objetivos de la organización se cumplan, así como determinar las implicaciones que se producen de los requisitos de la organización que se traducen en la compra de dispositivos e implementación de medidas.

La política de seguridad reúne los objetivos de la organización con respecto a la seguridad de sus sistemas e información, la misión y la visión de la misma, así como cuáles son los requisitos de la organización para implementar la seguridad como la adquisición de equipo especializado y sus configuraciones correspondientes para cada uno.

Tiene como objetivos informar las obligaciones para cada tipo de persona perteneciente a la organización, sus privilegios y alcances en el uso del sistema, definiendo las acciones que están permitidas y cuáles no. Define las consecuencias que tendría el suceso del algún accidente sobre la información y el funcionamiento de la organización, así como las reprimendas a tomar en caso de que se presente una acción no permitida. También se establece los pasos a seguir en caso de que se presente un ataque o daño a la integridad de la información y del

sistema mismo. Del mismo modo, la identificación de las vulnerabilidades y amenazas es importante, para saber de qué se protegerá al sistema, y la identificación de las herramientas que se utilizarán para mantener protegida la información, por medio de un análisis de riesgos.

La política de seguridad se presenta como un documento redactado de tal forma que sea entendible para todo el personal de la organización. Todos los involucrados en la organización deben tener claro cuáles son sus límites y cómo actuar en caso de presentarse problemas.

La elaboración de un plan de contingencias, procedimientos preventivos y correctivos está entre los objetivos establecidos en el documento de políticas de seguridad.

1.2.2.1 Plan de contingencias

Determinadas amenazas a cualquiera de los activos de un sistema de información pueden poner en peligro la continuidad de un negocio. El plan de contingencias es un instrumento de gestión de que contiene las medidas (tecnológicas, humanas y de organización) que garanticen la continuidad del negocio o proyecto protegiendo el sistema de información de los peligros que lo amenazan o recuperándolo tras un impacto.

El plan de contingencias consta de tres sub planes independientes:

- *Plan de respaldo.* Ante una amenaza, se aplican medidas preventivas para evitar que se produzca un daño. Por ejemplo, crear y conservar en un lugar seguro copias de seguridad de la información, instalar medidas físicas que cuiden las instalaciones como pararrayos, así como simulacros.
- *Plan de emergencia.* Contempla qué medidas tomar cuando se está presentando una amenaza o cuando acaba de producirse. Por ejemplo, restaurar de inmediato las copias de seguridad o activar el sistema automático de extinción de incendios.
- *Plan de recuperación.* Indica las medidas que se aplicarán cuando se ha producido un desastre. El objetivo es evaluar el impacto y regresar lo antes posible a un estado normal de funcionamiento del sistema y de la organización. Por ejemplo, tener un lugar alternativo donde continuar la actividad si el habitual hubiese sido destruido, sustituir el material deteriorado, reinstalar aplicaciones y restaurar copias de seguridad.

1.2.2.2 Procedimiento preventivo

Si hay un problema que es compartido, desde los grandes gobiernos, grandes corporaciones y hasta el usuario final es la falta de prevención. Siempre existe el pensamiento de que nunca sucederá un hecho que comprometa nuestros activos, y si sucede, no afectará de forma irrevertible.

Es importante cambiar la forma de pensar que un desastre "puede" ocurrir por el pensamiento de que el desastre "ya ha ocurrido". Este cambio de visión involucra un crecimiento que envuelve la forma en que se protegen los activos y las medidas tomadas para que no ocurran.

Se debe de pensar que un desastre en el sistema ha ocurrido y sobre el realizar un procedimiento preventivo que constará de políticas y acciones que nos permitan prevenirlo para que la posibilidad de ocurrencia sea escasa para que en el momento en el que realmente ocurra se cuenten con las medidas y herramientas necesarias para volver a poner en marcha el sistema a la normalidad.

El propósito de un procedimiento es describir todas las actividades relacionadas con la iniciación, implementación y almacenamiento de acciones preventivas.

Los ISO 27000 y 28000 tratan sobre los procesos para la creación de procedimientos preventivos.

1.2.2.3 Procedimiento correctivo

El propósito de un procedimiento correctivo es describir todas las actividades relacionadas con la iniciación, implementación y almacenamiento de acciones correctivas ante un desastre o ataque al sistema.

Un procedimiento correctivo reduce el efecto de un ataque. Respaldos de datos, planes de recuperación ante desastres y la disponibilidad de dispositivos de hardware redundante son ejemplos de procedimientos de corrección.

La detección de actividades tiene la capacidad de reconocer ataques y ponen en marcha contramedidas o procedimientos correctivos. Por ejemplo, los antivirus detectan virus que entran al sistema y pueden realizar procedimientos correctivos tales como remover los virus y poner en cuarentena los archivos infectados. El uso de software de monitorización para hacer seguimiento de usuarios, actualizaciones de archivos, y cambios críticos en el sistema pueden también ayudar a detectar anomalías que indican una intrusión o una amenaza.

1.2.3 Firewalls

Un firewall es un dispositivo que está conectado entre dos redes de datos y aplica una política de seguridad. Esas dos redes a las que está conectado el firewall son la red confiable (la red local) y la red no confiable (una red externa, usualmente Internet), figura 1.23. La tarea principal del firewall es proteger a la red confiable de la red que no lo es y esto lo hace a través de reglas establecidas, ya sea para permitir todo el tráfico que sale de la red confiable a la red no confiable, y permitir sólo las conexiones autorizadas de la red no confiable a la red confiable.

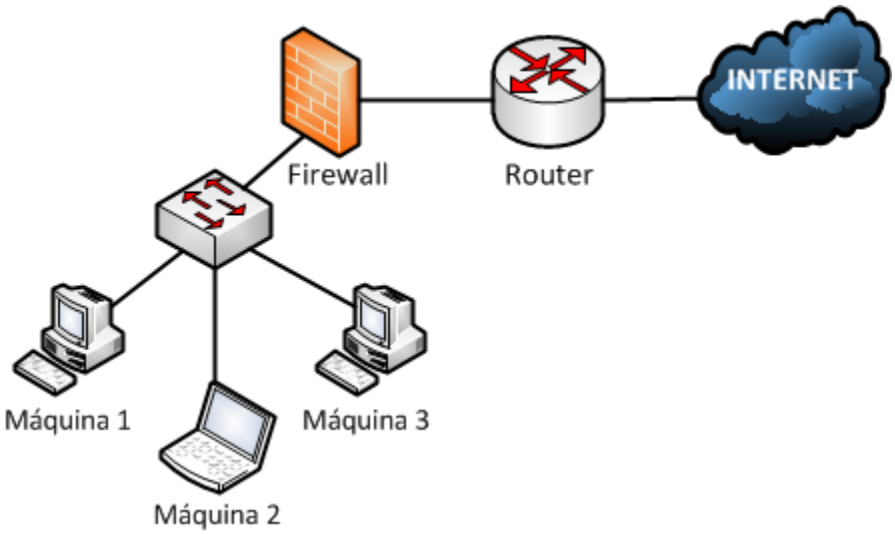

Figura 1.23. Conexión de firewall en una red local.

En la figura anterior se muestra la ubicación de un firewall en la red. Este se encuentra conectado entre el Switch (que interconecta a los dispositivos de la red local) y el Router (que rutea los paquetes generados por la red local hacia Internet). Se elige la implementación de un firewall en una red porque es un dispositivo que ofrecerá seguridad en la misma ya que impedirá que se realicen conexiones desde exterior, prevendrá accesos no autorizados, bloqueará el acceso puertos de comunicación que estén abiertos en algún equipo de la red local para que no se aproveche la vulnerabilidad, entre otras ventajas. Se ubica antes del Router para que el tráfico de la red local sea filtrado y entregado tal como se desea según las reglas del firewall al Router, y así restarle a este último carga de trabajo asimismo, si el Router permitió una solicitud de conexión a un equipo de la red local a un dispositivo desde Internet, el firewall detendrá que se lleve a cabo la comunicación.

El firewall funciona sobre la capas de enlace, la capa de red, la capa de transporte y de la capa de aplicación del modelo OSI. Se debe de tener en claro los objetivos de seguridad de la organización para poder elegir la mejor herramienta y las reglas de filtrado que utilizará el dispositivo para proteger la red.

Los firewalls de red hacen uso de los *puertos de red*, direcciones MAC, direcciones de red IP y protocolos de red para realizar la elección de los paquetes permitidos y cuáles no. Se pueden negar el acceso a ciertos puertos de los servicios ofrecidos por el sistema de información, por ejemplo, denegación de acceso a la conexión remota a través del puerto 22 de SSH (*Secure Shell, Shell Segura*). Un Router podría efectuar estas mismas tareas con la debida configuración.

Sin embargo, un firewall de aplicación implementa mayores opciones para brindar seguridad, y por lo tanto exige mayor trabajo al dispositivo donde se implementará. Además de controlar el acceso por medio de puertos y direcciones de red, es posible controlar sesiones y protocolos, por ejemplo, se puede establecer que no haya acceso por medio del protocolo ftp (protocolo de transferencia de archivos) no importando el puerto utilizado.

Las reglas en el firewalls son cadenas que establecen las acciones a realizar por el dispositivo. Cada paquete que pasa por el firewall proporciona información en su cabecera que es buscada en la lista, en caso de encontrar coincidencia, se permite que salga o entre de la red, en el caso permisivo o se rechaza el paquete eliminándose en el caso de denegación.

Hay dos formas básicas para iniciar a construir la lista de acciones que revisará el firewall para el control del tráfico en la red:

- Negar todo de manera predeterminada, permitir sólo los paquetes seleccionados.
- Aceptar todo de manera predeterminada, denegar sólo los paquetes seleccionados.

La primera de las opciones es la más acertada, debido a que se tiene todo negado, sólo se tiene que identificar bien los servicios que se necesitan dentro de la organización para permitir el trabajo interno. En cambio, la segunda opción establece una forma más fácil para echar a andar el firewall; no obstante, se podrían negar ciertos tipos de paquetes, pero sin tener cabalmente todas las opciones restringidas dejando huecos inseguros hasta que sea demasiado tarde.

1.2.3.1 Tipos de firewalls

- **Filtrado de paquetes**

Un firewall es el encargado de filtrar paquetes basados en los siguientes criterios de filtrado:

- Protocolos de red utilizados.
- Direcciones IP de origen y de destino.
- Puertos de origen y de destino.

Como se puede notar, este firewall trabaja sobre las capas de red y de transporte del modelo OSI. Entre las ventajas que ofrece es que son económicos, ofrecen un alto desempeño y los usuarios no saben de su existencia en la red ya que este es transparente a ellos.

Entre las desventajas que tienen es que no protegen a un nivel de capas superiores del modelo OSI y no son capaces de ocultar la topología de la red al exterior.

- **Firewall Dual-Homed**

Estos dispositivos están conectados a las dos redes de datos; sin embargo, no tiene habilitada la función de reenvío de paquetes, por lo cual, para poder hacer uso de un recurso de una red no confiable desde la red local, es necesario realizar una conexión con el Firewall y este realizará una conexión con el servicio exterior solicitado creando un puente entre el usuario local y el servicio exterior.

- **Screened host**

Esta implementación utiliza el filtrado de paquetes para mantener a la red interna aislada; sin embargo, sólo se tendrá a un dispositivo accesible desde el exterior a él, mientras tanto, en la red interna se filtrarán los paquetes y sólo unos cuantos servicios serán permitidos para la red local, pero todos los dispositivos en esta se mantendrán inaccesibles desde el exterior. Usualmente, el equipo que es accesible desde internet es llamado "*host de bastión*" y se trata de una computadora de propósito general en una red diseñada para resistir ataques, mientras este equipo está totalmente expuesto a ataques, véase figura 1.24.

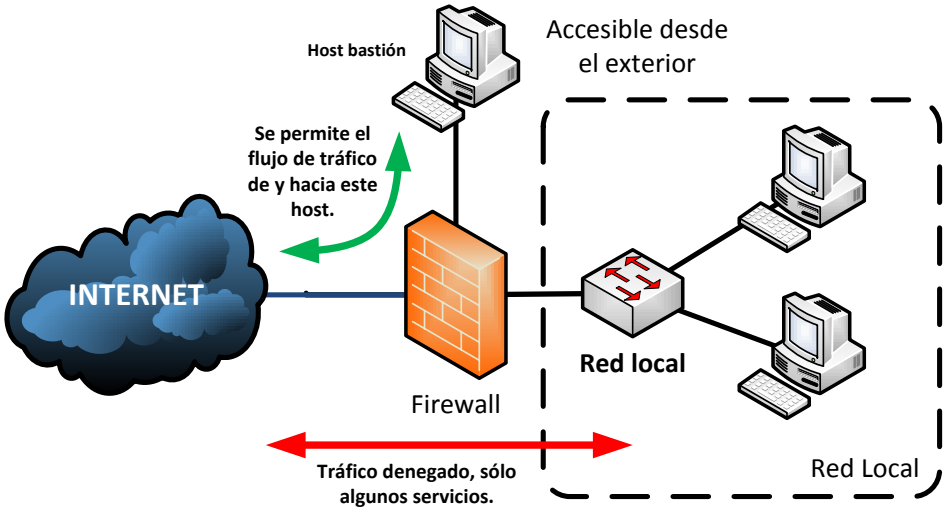

Figura 1.24. Firewall Screened-Host

- **Screened subnet**

El firewall *Screened subnet* es una variación de los firewalls de filtrado de paquetes y del firewall *dual-homed*. Puede ser usado para separar componentes de la red en pequeños sistemas, alcanzando un mayor rendimiento y flexibilidad. Cada componente del sistema de este firewall necesita implementar únicamente una tarea, cada sistema es menos complejo para configurar.

La forma de conexión de este tipo de firewall es como la que se presenta a continuación: se utilizan dos firewalls, uno se va a considerar interno y otro externo; sin embargo, el firewall externo se encargará de filtrar el tráfico de Internet hacia la red local y hacia el host de bastión; sin embargo, para evitar que intrusos ingresen a la red interna desde el host de bastión, el firewall externo se encargará de filtrar el tráfico que se genere del host bastión hacia la red interna.

Lo descrito en los párrafos anteriores queda plasmado en la figura 1.25.

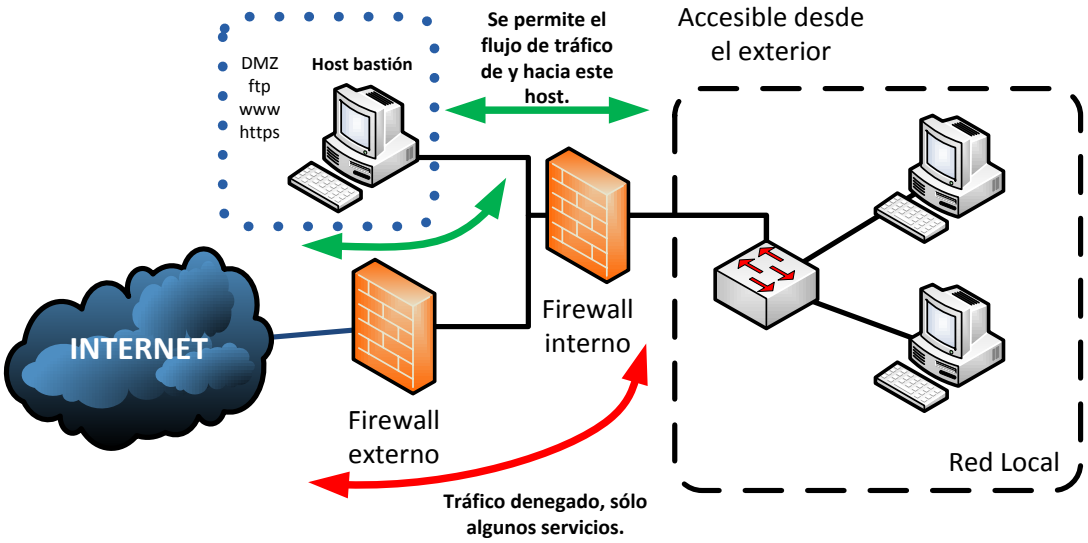

Figura 1.25. Firewall Screened subnet.

1.2.4 OpenBSD

OpenBSD surge dentro del desarrollo de NetBSD dejando a la seguridad como razón principal para la existencia de OpenBSD. El trabajo de los desarrolladores de OpenBSD se basa en la portabilidad, estandarización, corrección, seguridad proactiva y criptografía integrada del sistema operativo.

OpenBSD es un derivado del sistema BSD, por lo que hay muchas de las características de *UNIX* e incluso *Linux* en este sistema operativo, pero con sus características propias, no es una copia de ellos. Su principal tópico es la implementación de la seguridad en sistemas de información y redes de datos.

Su lema es "*Libre, Funcional y Seguro*" ya que cuenta con una licencia que permite al usuario trabajar con él libremente (distribuir, vender, dar, modificar, usar) y tiene diversas funcionalidades respecto a la seguridad de las redes y sistemas.

Aunque OpenBSD es capaz de ofrecer una Interfaz Gráfica de Usuario y herramientas de ofimática, la principal característica que lo vuelve un sistema operativo muy utilizado en ambientes empresariales son la variedad de servicios que proporciona para la implementación de redes de datos y la seguridad de la misma.

OpenBSD tiene la capacidad de implementar sobre él excelentes servicios de seguridad como firewalls, bridges o clasificadores de tráfico. Puede ser utilizado para soportar *NAT*, monitorización de tráfico y balance de cargas. Tiene integrado un firewall llamado PF (*Packet Filter, Filtrador de paquetes*) que permite la administración y control del tráfico que existe en la red. La seguridad que tiene por defecto es totalmente estricta rechazando el tráfico a todos los puertos excepto al 22 (puerto de Secure Shell SSH), detiene tantos servicios como sea posible y todos los demonios configurados de forma segura, manteniendo los no relevantes desactivados.

1.2.4.1 Servicios en OpenBSD

NAT (*Network Address Traslation, Traductor de Direcciones de Red*) es servicio en un firewall que permite a un dispositivo o varios dentro de una red local (red privada) actuar como un agente entre Internet (una red pública) logrando su comunicación entre sí. Las redes locales siempre usan direcciones IP privadas, las cuales no pueden

usarse para comunicarse con otras redes en el exterior, sólo los dispositivos dentro de la red tiene comunicación; sin embargo, NAT tiene la capacidad de transformar las direcciones privadas en direcciones públicas para permitir la comunicación y flujo de datos al exterior de la red local. Todos los host en la red utilizarán la misma dirección pública al exterior, o utilizar un grupo de direcciones (*pool*), en el que cada una de las direcciones NAT soportará cierto número de traducciones. En la figura 1.26 se puede observar la conexión de una red a un equipo que ejecuta NAT.

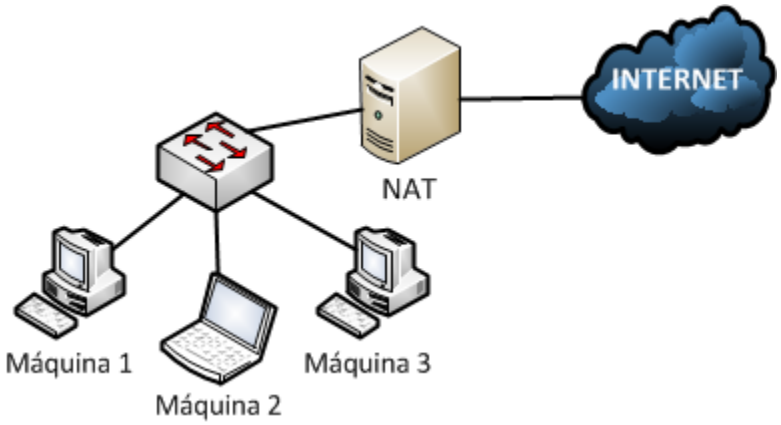

Figura 1.26. NAT en la red con OpenBSD

1.2.4.2 Balance de cargas

Cuando se tiene una empresa con un número grande de host en la red, es necesario contar con un pool de direcciones NAT para lograr dar un buen servicio a todos los dispositivos de la red. En estos casos, la dirección de origen dentro de la LAN se traducirá en una de las direcciones de la reserva, basándose en cierto método. Se utiliza el balanceo de cargas para evitar que alguna de las direcciones en el pool de NAT se congestione y deje de ofrecer un buen servicio, tanto para tráfico de entrada y de salida, distribuyendo las conexiones a través de todas las direcciones disponibles. Véase en la figura 1.27 un ejemplo de balanceo de cargas.

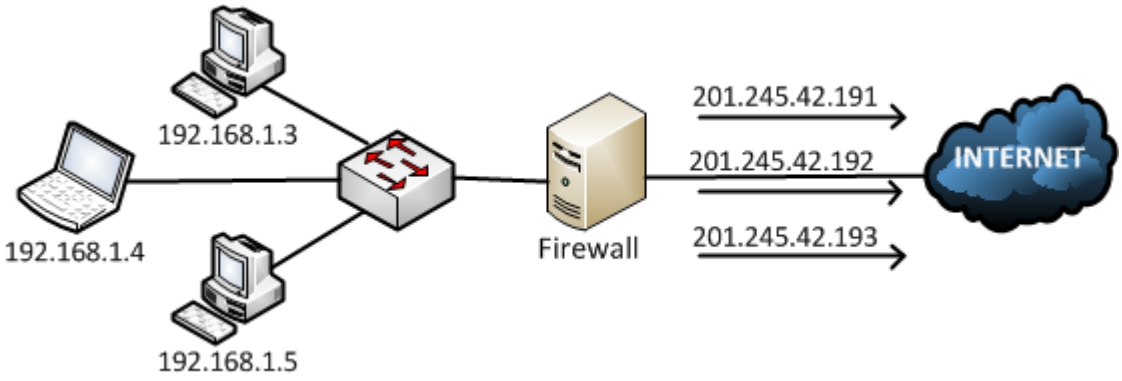

Figura 1.27. Balance de cargas en la red con OpenBSD

1.2.4.3 Bridge

El servicio de *Bridge* en un firewall lo hace como un enlace entre la red local de la organización y las redes externas. La transferencia de paquetes a través del bridge es transparente “invisible”, los dos segmentos de red que se encuentran unidos por el Bridge parecen ser uno. El puente sólo permite el flujo de ciertos paquetes de un

extremo al otro, esto hace que el tráfico en la red se reduzca, pues sólo podrá haber flujo de aquel tráfico que sea especificado.

Por las características del Bridge, el host dónde se esté ejecutando deberá tener dos interfaces físicas para conectar ambos segmentos, pero dada la acción que realiza, no tiene una dirección IP asignada a sus interfaces. Por esta razón el Bridge no puede ser administrado remotamente en caso de fallas y no puede funcionar como salida a Internet para una red Local, por esta razón, las direcciones de los dispositivos en la red local tiene que ser públicas para permitir conectarse con el exterior. Figura 1.28

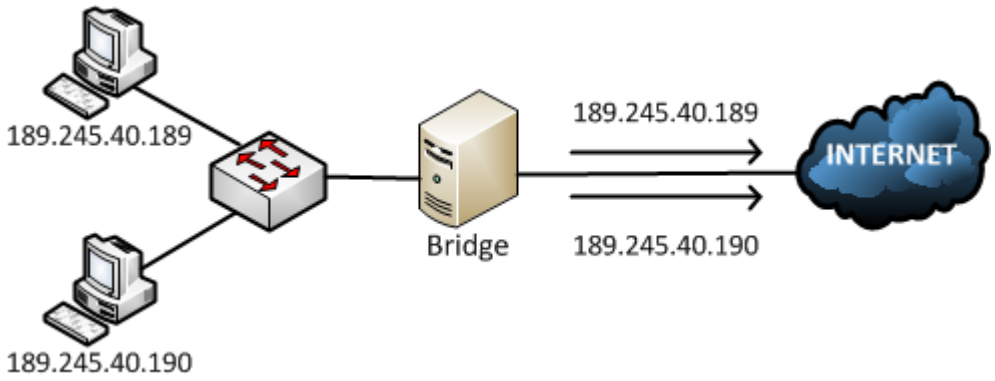

Figura 1.28. Bridge en la red con OpenBSD

OpenBSD ofrece diferentes servicios que permiten la administración de la seguridad en un sistema de información conectado a Internet, además de ser libre y barato.

1.2.5 PfSense

PfSense es una distribución personalizada de código abierto de FreeBSD adaptado para ser usado como firewall y Router en la red. Además de ser una plataforma muy poderosa como firewall y sistema de ruteo, tiene varias características que permiten crecer la seguridad de los sistemas sin tener que agregar más y evitar acrecentar el número de vulnerabilidades de seguridad a la distribución.

Las características que componen a PfSense que lo convierten en una opción viable para la protección de la red y administración de la misma son:

Firewall

Capaz de filtrar paquetes por direcciones de origen y destino, protocolos, puertos de origen y destino para tráfico TCP o UDP. Permite alta flexibilidad en la implementación de políticas posibles para la selección de puerta de enlace. Permite el balanceo de carga.

Tabla de estado

La tabla de estado del firewall mantiene información de las conexiones abiertas en la red. Gracias a características que toma de los *Packet Filter* de OpenBSD, PfSense logra mantener su tabla de estado con precisión.

Traductor de Direcciones de Red (NAT)

Capaz de utilizar un pool de direcciones públicas. Así también permite establecer una dirección pública para un host específico o una subred entera.

Redundancia

El protocolo *CARP* (*Common Address Redundancy Protocol, Protocolo de Redundancia de Dirección Común*) permite la creación de grupos de migración en entre dos o más firewalls. Si el firewalls principal falla en alguna de sus interfaces o totalmente, el firewall secundario se activa inmediatamente. PfSense incluye capacidad de sincronización, todo cambio de configuración en el firewall principal, se actualizan los firewalls secundarios.

Balanceo de carga

Permite el balanceo de carga para tráfico saliente con múltiples conexiones WAN en el que el tráfico se dirige al dispositivo de salida indicado o realizando un balanceo de carga sobre el pool de direcciones. También se puede realizar balanceo de carga para tráfico entrante para la distribución de carga entre diferentes servidores, usualmente servidores web y de correo, en caso de que alguno de los servidores falle a una solicitud *ping* se remueve del pool de servidores.

Redes Privadas Virtuales (VPN)

PfSense permite la implementación de conectividad VPN por medio de las herramientas *IPSec*, *OpenVPN* y *PPTP*.

Reporte y monitorización

Permite seguir y monitorizar en tiempo real gráficamente el comportamiento del sistema: Utilización de CPU, rendimiento total estado de los firewalls, rendimiento individual para cada interfaz, índice de paquetes por segundo para todas las interfaces, tiempos de respuesta a las puertas de enlace WAN.

DNS Dinámico y servidor DHCP

PfSense tiene incluido un cliente para DNS dinámico que permite el registro de la dirección IP pública una serie de proveedores de DNS dinámico. Asimismo, incluye las funcionalidades de servidor DHCP.

1.2.6 Listas de Control de Acceso (ACL)

Cuando se desea restringir el tráfico de datos de una red a otra se pueden utilizar Listas de Control de Acceso (ACL). Una ACL es una lista de sentencias permisivas o de denegación que se asignan a las interfaces del Router. Hay diferentes tipos de ACL entre las que se encuentran las listas de control de acceso estándar, las extendidas y las nombradas.

Una ACL estándar solamente puede denegar o permitir el tráfico de una IP origen. Dado que sólo se conoce la dirección IP origen, estás ACL se configuran cerca del destino. Estás ACL pueden permitir o denegar mucho. Estás listas de control de acceso son utilizadas en la implementación de NAT, telnet y VPN. En la configuración de una ACL estándar se pueden utilizar los números del 1 al 99.

Las ACL extendidas son eficaces debido a que estas permiten o deniegan tráfico de datos basándose en las direcciones IP de origen, de destino, protocolo de comunicación utilizado, número de puerto, e incluso, tiempos del día. Estás ACL tienen la dirección IP origen y la dirección IP destino por lo que estas listas son colocadas lo más cerca de la fuente para un funcionamiento correcto. Cuando un paquete trata de tener acceso a la red, este tiene como datos importantes en su cabecera las direcciones IP de origen y destino. Si la lista de acceso está configurada lo más cerca al origen, el paquete puede ser examinado sin la necesidad de generar tráfico extra en la red. Para la configuración de ACL extendidas se utilizan número de 100 al 199.

Las ACL nombradas son las más poderosas y más usadas para el control de acceso. Estas ACL permiten agregar secuencias de números a las sentencias de la lista, además de reemplazar los números en la configuración por

nombres. La secuencia de número permite borrar sentencias de la ACL sin eliminar la lista completa. Asimismo, como una ACL extendida, las listas de control de acceso nombradas son ubicadas cerca del origen.

2

Routing

2.1 La red del Instituto de Educación Media Superior del Distrito Federal

El Instituto de Educación Media Superior del Distrito Federal (IEMS) cuenta con 20 planteles y oficinas centrales, dada una de ellas representa una red independiente dentro de la misma organización.

La administración de red de los planteles es difícil debido a su distribución física y lógica, la resolución de problemas de red se realiza por medio de visitas a los cuartos de telecomunicaciones que presentan problemas y resolverlos internamente. También, el monitorización de las redes no se lleva a cabo de manera centralizada, cada uno de los planteles debe por su cuenta implementar las soluciones que le permitan monitorizar la red, así como la detección de anomalías.

La red del IEMS optimizará su direccionamiento de red a través de la división de subredes y la configuración de equipos de red que permitan tener una administración centralizada que admita la fácil resolución de problemas y monitorización de la red. El diseño del direccionamiento implica el diseño también de las conexiones entre los dispositivos. Las conexiones serán por medio de enlaces LAN-to-LAN.

La nueva infraestructura física será configurada con un direccionamiento que permitirá tener una red por medio de puertos extendidos que facilitará su administración y monitorización de recursos. Los dispositivos en cada plantel compartirán características en la configuración con el fin de mantener una red homogénea. Las oficinas centrales funcionarán como Centro de Operación de la Red en el que se llevará a cabo el monitorización de la red institucional, así como solución de problemas por medio de gestión remota.

2.2 Cálculo de subredes con VLSM

Para lograr que los 20 planteles y las oficinas centrales que conforman la red institucional del IEMS funcionen como una red unificada, se debe compartir el espacio de direccionamiento, es decir, a partir de una dirección IP privada, generar subredes que cumplan con los requerimientos de direcciones requeridas por cada plantel.

Actualmente cada plantel requiere 200 equipos funcionando en su red local aproximadamente, mientras que en las oficinas centrales del IEMS requieren un número similar de dispositivos funcionando. Por esta razón se propone el direccionamiento a utilizar en la implementación de la red de datos por puerto extendido con el uso de VLSM porque las redes en la institución son de diferentes tamaños, algunas redes con 50 usuarios, otras más con un poco más de 200 usuarios. VLSM permitirá que el direccionamiento se proveche de una excelente manera y exista muy poco desperdicio de IP (ocurre desperdicio cuando se tiene un gran número de direcciones IP que no se utilizan porque no el número de dispositivos conectados no utilizan ni el 50% del direccionamiento asignado). Cada vez que se requiera direccionamiento para un plantel, se le ofrecerá el número de direcciones IP que se necesitan.

El espacio de direccionamiento que se propone en este documento es un segmento de red 172.16.0..0/16 de clase B del bloque de direcciones IP privadas. Esta dirección cuenta con la máscara de clase 255.255.0.0 que proporciona 65, 536 direcciones IP (2^{16}). Se pudo haber utilizado cualquier otro segmento privado de direccionamiento, no existe ningún problema si se utiliza cualquiera de los segmentos privados de las clases A, B y C de direcciones IP; sin embargo, si se elige un segmento de red de la clase proferida, se recomienda que se elija solo direccionamiento de dicha clase y así mantener homogéneo el direccionamiento, esto con el fin de ayudar a la sumarización de redes en un futuro y optimizar las actualizaciones del protocolo de ruteo que se implemente.

Se toma como partida el segmento de red 172.16.0.0/16 para iniciar la división de subredes y se obtienen los segmentos que serán asignados a cada plantel.

Tabla 2.1. Direccionamiento de las redes de los planteles

Plantel	Dirección de red calculada con VLSM con prefijo CIDR	Máscara de subred
Plantel 1	172.16.1.0/24	255.255.255.0
Plantel 2	172.16.2.0/24	255.255.255.0
Plantel 3	172.16.3.0/24	255.255.255.0
Plantel 4	172.16.4.0/24	255.255.255.0
Plantel 5	172.16.5.0/24	255.255.255.0
Plantel 6	172.16.6.0/24	255.255.255.0
Plantel 7	172.16.7.0/24	255.255.255.0
Plantel 8	172.16.8.0/24	255.255.255.0
Plantel 9	172.16.9.0/24	255.255.255.0
Plantel 10	172.16.10.0/24	255.255.255.0
Plantel 11	172.16.11.0/24	255.255.255.0
Plantel 12	172.16.12.0/24	255.255.255.0
Plantel 13	172.16.13.0/24	255.255.255.0
Plantel 14	172.16.14.0/24	255.255.255.0
Plantel 15	172.16.15.0/24	255.255.255.0
Plantel 16	172.16.16.0/24	255.255.255.0
Plantel 17	172.16.17.0/24	255.255.255.0
Plantel 18	172.16.18.0/24	255.255.255.0
Plantel 19	172.16.19.0/24	255.255.255.0
Plantel 20	172.16.20.0/24	255.255.255.0

El número de bits utilizados para la porción de red es de 24 bits, tomando 8 bits restantes para la generación de 254 direcciones de hosts utilizables.

Cada una de las subredes cuenta con 254 direcciones de red disponibles para configuración de equipos que se conectarán a la LAN correspondiente. Cada red configurará estas direcciones de manera estática, manualmente o dinámicamente por medio de un servidor DHCP dedicado o a través del Router que se utilizará de enlace de la red con el exterior. La red 172.16.0.0/16 se utilizó hasta llegar a la dirección de red utilizable 172.16.20.0/24; sin embargo, es necesario utilizar direcciones de red para los enlaces entre Routers que enlazan a cada plantel con el Router que direccionará el tráfico de las redes a Internet.

Esos enlaces requieren sólo dos direcciones IP, la dirección IP de la interfaz del Router del plantel y la dirección del enlace WAN al Router principal. Por esta razón, el número de bits a utilizar en la porción de host es de dos, que nos proporciona cuatro direcciones de host ($2^2 = 4$), de las cuales, una es la dirección que identifica a la red, dos direcciones utilizables, y la dirección de broadcast. Esta división de subredes empieza desde la dirección 172.16.21.0/24, segmentos que quedan de la división de subredes realizada para los planteles.

Tabla 2.2. Direccionamiento de los enlaces WAN sin consideración de expansión futura

Enlace con Router de enlace	Dirección de red calculada con VLSM con prefijo CIDR	Máscara de subred
Plantel 1	172.16.21.0/30	255.255.255.252
Plantel 2	172.16.21.4/30	255.255.255.252
Plantel 3	172.16.21.8/30	255.255.255.252
Plantel 4	172.16.21.12/30	255.255.255.252
Plantel 5	172.16.21.16/30	255.255.255.252
<Se omiten más datos>		

Sin embargo, las redes mostradas en la tabla anterior ya no permiten tener un direccionamiento contiguo en caso de que exista la posibilidad de crear más planteles, así que se toma un margen de direcciones considerando el crecimiento futuro de la institución. El espacio de direcciones que se propone utilizar inicia con la red 172.16.30.0/24 la cual es dividida en subredes con dos direcciones de red útiles, sólo ese número de direcciones IP porque sólo se necesitan la dirección IP del dispositivo que conecta al plantel y el dispositivo central.

Tabla 2.3. Direccionamiento de los enlaces WAN

Enlace con Router de salida	Dirección de red calculada con VLSM con prefijo CIDR	Máscara de subred
Plantel 1	172.16.30.0/30	255.255.255.252
Plantel 2	172.16.30.4/30	255.255.255.252
Plantel 3	172.16.30.8/30	255.255.255.252
Plantel 4	172.16.30.12/30	255.255.255.252
Plantel 5	172.16.30.16/30	255.255.255.252
Plantel 6	172.16.30.20/30	255.255.255.252
Plantel 7	172.16.30.24/30	255.255.255.252
Plantel 8	172.16.30.28/30	255.255.255.252
Plantel 9	172.16.30.32/30	255.255.255.252
Plantel 10	172.16.30.36/30	255.255.255.252
Plantel 11	172.16.30.40/30	255.255.255.252
Plantel 12	172.16.30.44/30	255.255.255.252
Plantel 13	172.16.30.48/30	255.255.255.252
Plantel 14	172.16.30.52/30	255.255.255.252
Plantel 15	172.16.30.56/30	255.255.255.252
Plantel 16	172.16.30.60/30	255.255.255.252
Plantel 17	172.16.30.64/30	255.255.255.252
Plantel 18	172.16.30.68/30	255.255.255.252
Plantel 19	172.16.30.72/30	255.255.255.252
Plantel 20	172.16.30.76/30	255.255.255.252

La tabla anterior muestra las direcciones de red que se configurarán en los enlaces entre los Routers de los planteles, así como permitir la comunicación entre las redes locales. La configuración de los enlaces se hará sobre VLAN y la comunicación entre las mismas por medio de la configuración del Router-on-a-stick. La asignación de las direcciones IP se propone la siguiente: la más alta en el rango se le asignará al Router del plantel mientras que la más baja se configurará en la interfaz del dispositivo central.

Las oficinas centrales del IEMS necesitan tres segmentos de red, mismas que se dejarán con tres segmentos de red de clase C con 254 direcciones de red disponibles cada una. Estas subredes no se encuentran dentro de los bloques privados de clase B porque no son planteles, sólo se buscará que el direccionamiento de planteles esté en la clase B, mientras que la de las oficinas centrales serán clase C y así mantener diferenciado el tráfico. Estás subredes son las siguientes:

- Subred 1: Segmento de red 192.168.1.0 con máscara de subred 255.255.255.0
- Subred 2: Segmento de red 192.168.2.0 con máscara de subred 255.255.255.0
- Subred 3: Segmento de red 192.168.3.0 con máscara de subred 255.255.255.0

2.3 Conexión física de los planteles

La manera en que las redes locales en cada uno de los planteles de la Institución educativa se conectaban a Internet era a través de un módem conectado a la línea de DSL que les proporcionaba acceso. Actualmente con la propuesta de este proyecto, cada red local forma parte de una red única, jerarquizada y que gracias a las mejoras proporcionan una red administrable y escalable. Mucho de ello depende en gran medida de la conexión física que se tratará a continuación.

2.3.1 Puertos extendidos

La red institucional del IEMS se compone de varias subredes que están distribuidas geográficamente. Para los administradores de red, comunicar cada una las subredes que forman la red puede realizarse de diversas maneras, y esto dependerá en gran medida del proveedor de servicios, la seguridad que se desee implementar al tráfico de datos y el presupuesto que se cuente para el proyecto.

Este proyecto está destinado a resolver los siguientes problemas presentados en la red de la Institución:

- Cada red local en los diferentes planteles de la Institución es una red de datos independientes, difícil de gestionarse y sin un esquema de seguridad adecuado. Asimismo, la monitorización de los dispositivos no se lleva a cabo por un ente centralizado que detecte fallas rápidamente.
- El caso de utilizarse Internet para la comunicación entre los planteles, las principales desventajas se encuentran en la seguridad de la información y la velocidad de transmisión utilizada. Dado que la infraestructura de Internet es pública, los datos que se transportan a través de ella pueden ser blanco de ataques informáticos, por ejemplo, una intercepción y/o modificación de la información. Asimismo, la utilización de Internet añade un retardo por cada dispositivo de la red pública en la que la información se transporta.

Sin embargo, una de las metas que se establecen en este proyecto es que la infraestructura de la red permita que esta sea administrable en un solo punto, y que el tráfico de la red entera hacia Internet tenga un solo punto de salida. De la misma forma, se busca que todas las subredes conectadas funcionen como una red LAN a pesar de no estar ubicadas en un mismo lugar geográfico.

Para lograr la infraestructura planeada, cada una de las redes LAN se extenderá a las otras en un punto por medio de enlaces LAN-to-LAN (L2L), conocida también como “Puertos Extendidos”. Un puerto extendido permite la conexión de una red LAN con otra red LAN distribuidas geográficamente como si estuvieran en un mismo edificio,

es decir, los dispositivos de ambas redes se comunicarán como si estuvieran en la misma red local sin importar la distancia, esto debido a la tecnología y capacidad que ofrece este tipo de enlace y con las ventajas que se tendrían, tal como si estuvieran conectadas ambas redes LAN directamente sin distancias geográficas. Por esa razón a esta solución se le llama conexión por *puertos extendidos*, es tal la ventaja que ofrecen que es como si los puertos (interfaces) de los dos equipos se extendieran y conectaran.

Las características que ofrecen los enlaces LAN-to-LAN son las siguientes:

- Se proporciona una conectividad Ethernet, es decir, por medio de la infraestructura física que construye por el proveedor de servicios frece conectividad Ethernet a nivel de capa 2 transparente y totalmente dedicada. Un enlace L2L conecta dos extremos del mismo cliente sin necesidad de configurar protocolos adicionales por parte del proveedor. Los protocolos que utilice el usuario, así como configuración de direccionamiento son configurados como se harían en un entorno local de manera normal.
- Alta velocidad de 1 Gbps hasta 2 Gbps capaces de transportar gran volumen de tráfico.
- Infraestructura: Los enlaces dedicados LAN-to-LAN proporciona los equipos de terminación de red (NTU) para colocarse en ambos extremos del enlace para ofrecer una interfaz de acuerdo al tipo de conexión (fibra óptica o Ethernet RJ-45) sin la necesidad de instalación de equipo adicional para la conversión de protocolos.
- Independencia de la distancia: Las aplicaciones y comunicación que se realiza entre los extremos conectados por medio del enlace funcionarán de la misma manera y a la misma velocidad tal como si los equipos estuvieran ubicados en el mismo cuarto de comunicaciones. Por esa razón, este tipo de enlaces son conocidos como “Puertos extendidos”, así como si uno de los puertos fuera prolongado de un lugar a otro.

Las ventajas que trae consigo el uso de enlaces LAN-to-LAN son:

- Servicio económico: el uso de la infraestructura LAN-to-LAN que ofrece el proveedor se paga de manera mensual o trimestral, permitiendo manejar de manera sencilla el control del presupuesto. Asimismo, debido a que son enlaces dedicados, no se invierte en las soluciones de seguridad en todos los puntos, sino que se plantean puntos estratégicos para su implementación, reduciendo costos.
- Funcionalidad unificada: Los usuarios de los planteles conectados mediante los enlaces L2L podrán comunicarse y acceder a la información como si se estuviera en una única red, compartir aplicaciones desde cualquier ubicación como si se tratase de un servicio local.
- Flexibilidad: Debido a que los enlaces L2L son transparentes a los protocolos y la solución de conectividad es escalable, se puede hacer uso del ancho de banda que se ajuste las necesidades simplemente haciendo la petición al proveedor y realizando el ajuste al presupuesto.
- Seguridad: Debido a que el transporte de datos se realiza por medio de enlaces dedicados, no hay transporte de los datos a través de Internet, haciendo una transferencia confiable de la información.
- Las interfaces físicas en los extremos son sencillas que van desde conectores de fibra óptica a RJ-45. Esto elimina la complejidad del uso de interfaces usadas por el uso de ATM o SDH.

2.3.2 Conexión física de la red del IEMS

Para poder comprender la conexión física de los dispositivos a través de este nuevo diseño de red, se tienen que tratar diversos conceptos de importancia que están relacionados forzosamente con la infraestructura que se proporciona al cliente, en este caso el IEMS.

La conexión de la red local de cada uno de los planteles se puede realizar por medio de varios Switches que proporcionen la cantidad de puertos suficientes por medio de un arreglo en pila (stack). Sin embargo, la conexión del Router de cada plantel con el Router de enlace ubicado en las oficinas centrales es importante en su planeación. Los Routers de cada plantel se podrían conectar a una interfaz del Router de enlace como se muestra en la figura 2.1.

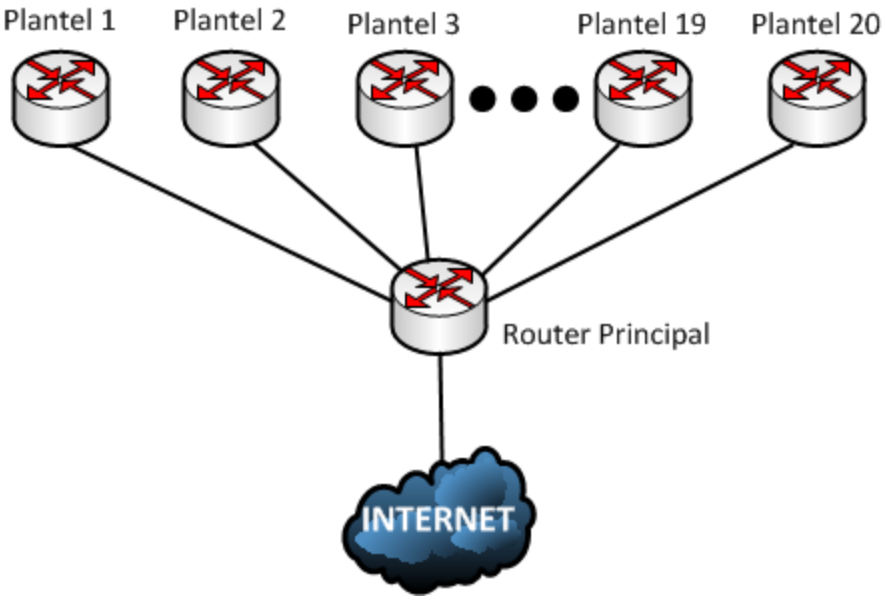

Figura 2.29. Conexión física entre planteles y Router principal

Los Routers no se caracterizan por tener numerosas interfaces, se necesitan 20 puertos para los planteles y un puerto conectado a la salida hacia Internet. El dispositivo que posee la característica de contar con un gran conjunto de puertos para dar servicio es el Switch, pero, un equipo de capa 2 como este no tiene la capacidad de enrutar paquetes a otros dispositivos fuera de la red local como lo haría un Router, al menos que se tratase de un Switch de capa 3, por el costo que tienen estos dispositivos, no se contempla en este documento.

La propuesta de la conexión física de los planteles con el Router que les dará salida a Internet se concebirá por medio de un Switch de alta velocidad que se encargará de recibir los enlaces y conectarlos al Router de salida de los planteles a través de un solo enlace con capacidad de soportar la cantidad de datos que se generarán, considerar la figura 2.2.

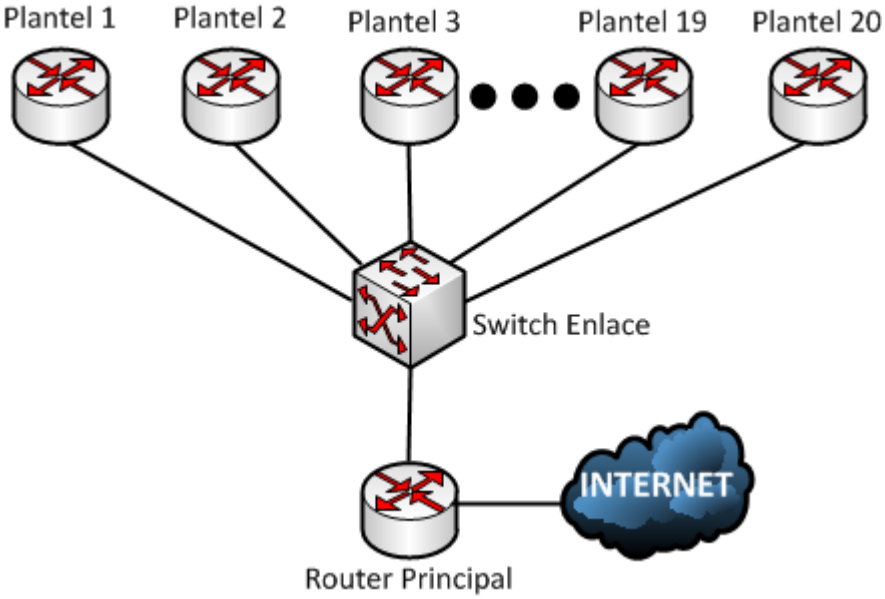

Figura 2.30. Propuesta de conexión de los planteles por medio de un Switch

Para que la conexión física que se propone funcione, es necesario planear la conexión lógica. La conexión lógica será posible utilizando Redes de Área Local Virtuales (VLAN), permitiendo que las redes de los planteles se puedan enlazar al Router de salida por medio de una sola conexión física. Esta interfaz puede ser dividida en interfaces virtuales con las mismas propiedades de un puerto físico en su configuración puesto que se le puede configurar una dirección IP con su respectiva máscara. Este tipo de interfaces virtuales son llamadas subinterfaces. Asimismo, las VLAN permitirán dividir en el Switch el tráfico en dominios de broadcast independientes.

El IEMS tiene en su inventario equipos de cómputo que pueden ser adecuados para ofrecer el servicio de Router de enlace, por lo que en lugar de hacer uso de dispositivos comerciales, el enlace de los planteles se realizará por medio de equipos de cómputo con el sistema operativo pfSense, que configurado correctamente, ofrecerá las características de un Router. Este equipo contará con dos interfaces de red, una de ellas estará conectada al enlace LAN-to-LAN y el otro al Switch de la red local. Es importante mencionar que la única característica que se plantea utilizar en los equipos de PfSense es la de Router (reenvío de paquetes) y no el de firewall, la implementación de la seguridad se implementará en la salida hacia Internet de toda la red, y así evitar carga adicional de procesamiento a los dispositivos que se ubicarán en los planteles. Ahora bien, también se proyecta una migración de los equipos PfSense por Routers comerciales y aprovechar las características que ofrecen los dispositivos, entre ellas, la más importante, la implementación de un protocolo de ruteo dinámico.

En cada plantel, el equipo con PfSense estará conectado a uno de los extremos del enlace LAN-to-LAN que el proveedor habrá dejado instalado con un conector RJ-45, por lo que, el extremo que va a las oficinas centrales también será un cable con conector RJ-45 conectado al Switch de enlaces.

Se presenta como una primera fase el uso de dispositivos sobre el sistema operativo PfSense ya que la compra de Routers comerciales representa un gasto de gran impacto para la institución, aunque representaría una infraestructura de red confiable y escalable, pero no se cuenta con el presupuesto suficiente para su compra, por lo que el uso de una herramienta libre y de gran funcionalidad como PfSense representa una solución eficaz. Sin embargo, la infraestructura y el diseño del direccionamiento permiten que en el futuro la instalación de Routers reemplazando a PfSense sea fácil y rápida, con impactos favorables a la red en cuestión de capacidad. En este documento se trata la configuración de los equipos y su integración a la red; a pesar de eso, el punto medular de este trabajo es la integración de una red con enrutadores, y la configuración de un protocolo de ruteo dinámico que proporcionen una red escalable, confiable y convergente.

La topología propuesta para la red local de las oficinas centrales es la siguiente mostrada en la figura 2.3.

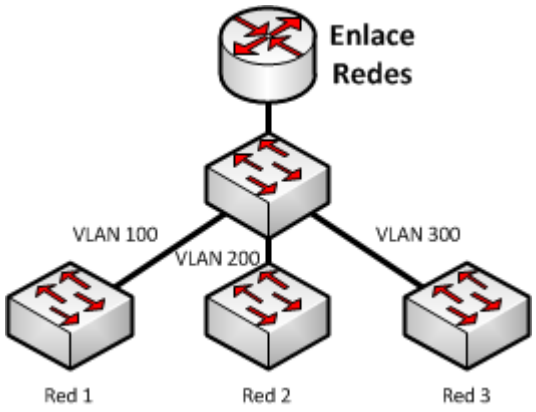

Figura 2.31. Red de las oficinas centrales

En las oficinas centrales se conectará un arreglo de Switches al Router que dará salida a la red local, mismos que darán acceso a los dispositivos de las tres redes. La segmentación de las redes en la red local de Switches se realizará por medio de la configuración de VLAN y enlaces troncales. El Switch que interconecta a cada uno de los Switches de los planteles estará conectado al Router por medio de un enlace troncal, y a la vez, estará conectado a los Switches de cada red por medio de un enlace configurado en una VLAN de acceso. La interfaz del Router estará dividida en subinterfaces para cada una de las VLAN en la red de las oficinas centrales.

Ambos Routers, el que conecta a los planteles con la red, como el dispositivo que hace lo propio con las oficinas centrales se conectarán entre sí por medio de un Switch que estará conectado a un dispositivo sobre OpenBSD (también puede ser utilizado un equipo sobre PfSense) de salida a Internet. Este Router OpenBSD estará conectado al enlace del proveedor a internet y es el único punto de salida para toda la red de datos del IEMS.

En la figura 2.4, la topología de la red completa de las interconexiones de las redes de la institución es la siguiente, los recuadros punteados representan los cuartos de telecomunicaciones en la que se encontrarán los dispositivos.

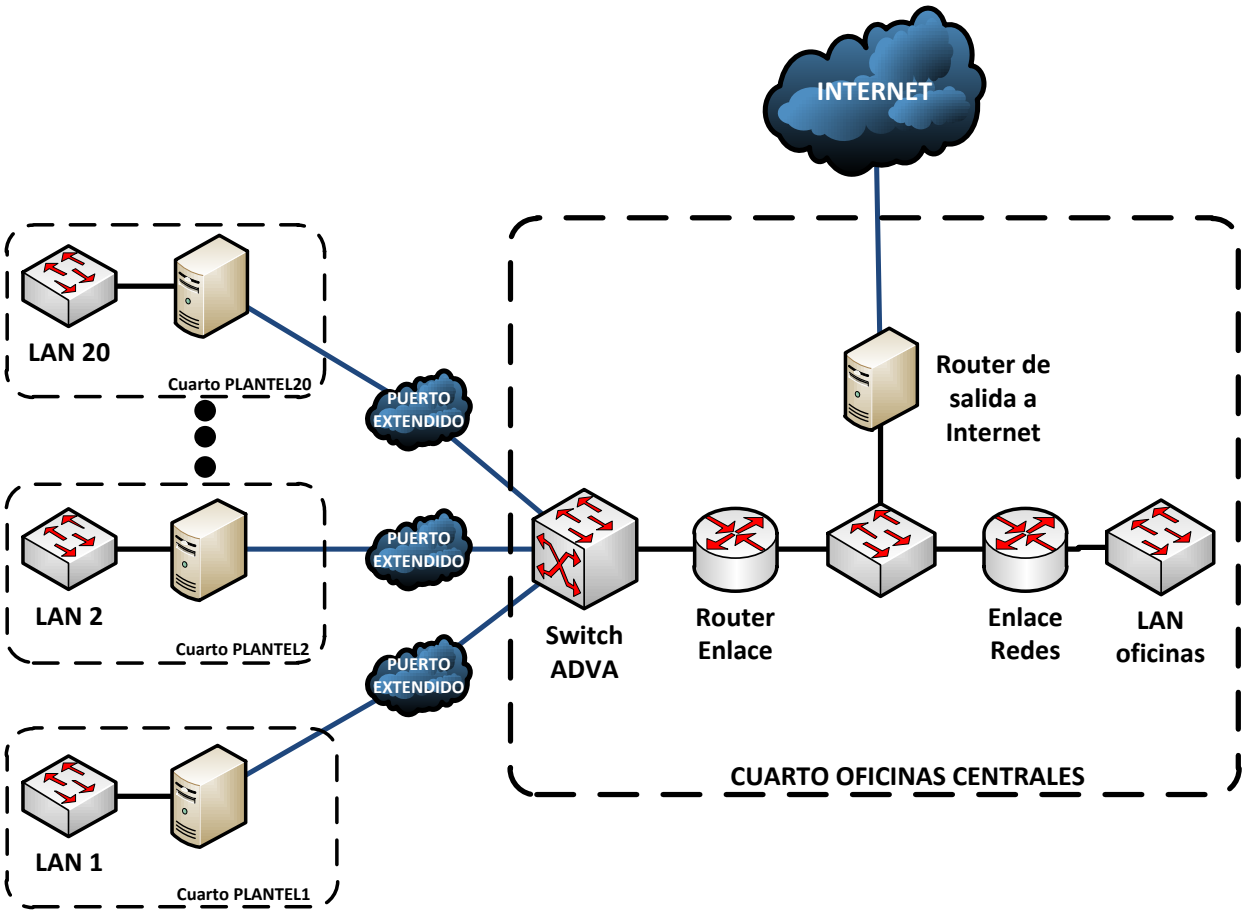

Figura 2.32. Topología completa propuesta para implementarse en la red del IEMS.

Esta estructura por medio de puertos extendidos y el uso de dispositivos con pfSense instalado brinda una red segura, funcional y económica. Estás tres características son importantes para la organización, que no cuenta con un presupuesto amplio para la compra de equipamiento nuevo de alguna marca líder en el mercado de dispositivos de

red, debido a que son soluciones caras. De cualquier forma, el diseño de la red permite que el ingreso de tecnología nueva sea fácil y con impactos positivos en la red.

El Router de enlace de los planteles tiene que ser forzosamente un dispositivo de red de alguna marca de dispositivos, por ejemplo, Cisco®. Esto porque es necesaria la configuración de subinterfaces para la comunicación entre VLAN. El Router de salida de las oficinas centrales también debe de ser un equipo especializado de red por el mismo motivo señalado para el Router enlace de planteles.

2.4 Asignación del direccionamiento en los planteles

La configuración del direccionamiento en el Router pfSense que conecta a la red del Plantel 9 será la siguiente: De la red 172.16.9.0/24 se tomará la dirección más alta en el rango de direcciones (172.16.9.254), que es la IP del equipo que permitirá la salida a la red local y se configurará en la interfaz que conecta a la red LAN del plantel. La dirección de red que conecta al Router pfSense con la red WAN será la última del rango en la red 172.16.30.32/30 en la interfaz específica.

Tabla 2.4. Asignación de direccionamiento en el equipo del plantel 9

Interfaz	Dirección de red	Función
LAN	172.16.9.254/24	Salida de la red local.
WAN	172.16.30.34/30	Conexión con el Router de Enlace

La configuración del enlace WAN es la siguiente, haciendo uso de la opción 2 del menú que es proporcionado por la interfaz de línea de comando de pfSense, como se puede observar en la figura 2.5.

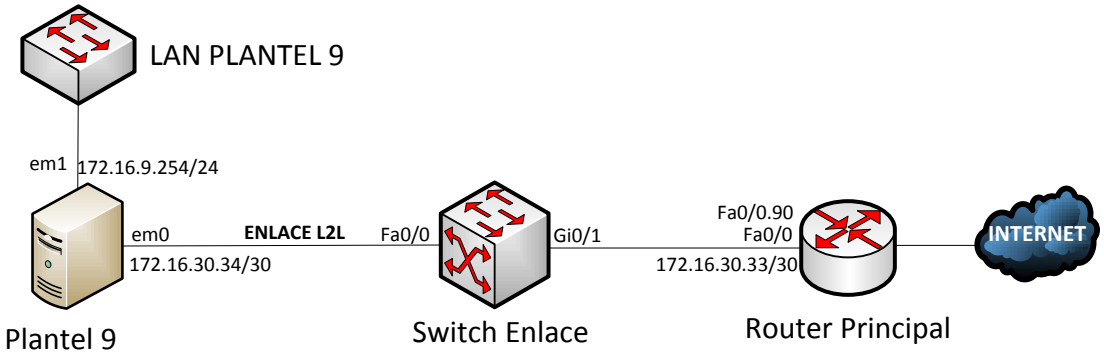

Figura 2.33. Diagrama de conexión del Plantel 9

Cuando ya se ha realizado la configuración de las interfaces de red, es necesaria también la realización de pruebas de conectividad con los extremos. Se ejecutará el comando PING en el equipo pfSense a la dirección IP de la subinterfaz que corresponde al plantel 9 en el Router principal. Esa dirección IP es la 172.16.30.33. Se ejecutará empleando la opción 7 del menú de la interfaz de comandos de pfSense. Esta petición deberá cruzar a través del enlace LAN-to-LAN hasta el Router principal que tendrá la función de Router-on-a-stick (está función se describirá más adelante). Figura 2.6.

```
 7) Ping host

Enter an option: 7


Enter a host name or IP address: 172.16.30.33

PING 172.16.30.33 (172.16.30.33): 56 data bytes
64 bytes from 172.16.30.33: icmp_seq=0 ttl=64 time=47.378 ms
64 bytes from 172.16.30.33: icmp_seq=1 ttl=64 time=0.203 ms
64 bytes from 172.16.30.33: icmp_seq=2 ttl=64 time=0.201 ms

--- 172.16.30.34 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.201/15.927/47.378/22.239 ms

Press ENTER to continue.
```

Figura 2.34 PING al Router de enlace

El comando ping fue satisfactorio, no hubo ningún paquete perdido o con retardo en su respuesta. Ahora se tiene que conectar a la interfaz LAN un Switch con un dispositivo para que por medio de DHCP reciba una dirección IP. Se verifica la IP que se le ha asignado por medio del comando *ipconfig* (equipo con sistema operativo Windows), figura 2.7. El comando ipconfig y el comando ifconfig en los sistemas UNIX despliegan información de la configuración de las interfaces de red de los equipos, como la dirección IP, máscara de subred, dirección IP del equipo que proporciona salida, dirección de los servidores de DNS, dirección MAC del dispositivo, entre otras cosas. Obsérvese figura 2.7.

```
Adaptador de Ethernet Conexión de área local:

   Sufijo DNS específico para la conexión. . : localdomain
   Vínculo: dirección IPv6 local. . . : fe80::b482:172a:d975:7d1d%11
   Dirección IPv4. . . . . . . . . . . . : 172.16.9.2
   Máscara de subred . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 172.16.9.254
```

Figura 2.35. Asignación de dirección IP a un equipo con sistema operativo Windows.

```
Configuración IP de Windows


Adaptador de Ethernet Conexión de área local:

   Sufijo DNS específico para la conexión. . : plantel9.iems.edu.mx
   Vínculo: dirección IPv6 local. . . : fe80::b482:172a:d975:7d1d%11
   Dirección IPv4. . . . . . . . . . . . : 10.30.9.12
   Máscara de subred . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 10.30.9.254
```

Figura 2.36. Parámetros por DHCP

Cada uno de los enlaces L2L que unen a los planteles con el Switch de alta velocidad se conectan él en un puerto, mismo que debe de estar configurado en una VLAN de acceso. Estos identificadores de VLAN deben de ser proporcionados por el proveedor de servicios ya que no se cuenta con la administración de ese dispositivo. Entonces, la VLAN 90 está dedicada al enlace entre el Router de salida al equipo pfSense del Plantel 9.

Tabla 2.5. Tabla de direccionamiento para Router pfSense.

Dispositivo	Interfaz	Dirección IP	Máscara de subred
PLANTEL 1	**Em0**	172.16.1.254	255.255.255.0
	Em1	172.16.30.2	255.255.255.252
PLANTEL 2	**Em0**	172.16.2.254	255.255.255.0
	Em1	172.16.30.6	255.255.255.252
PLANTEL 3	**Em0**	172.16.3.254	255.255.255.0
	Em1	172.16.30.10	255.255.255.252
PLANTEL 4	**Em0**	172.16.4.254	255.255.255.0
	Em1	172.16.30.14	255.255.255.252
PLANTEL 5	**Em0**	172.16.5.254	255.255.255.0
	Em1	172.16.30.18	255.255.255.252
PLANTEL 6	**Em0**	172.16.6.254	255.255.255.0
	Em1	172.16.30.22	255.255.255.252
PLANTEL 7	**Em0**	172.16.7.254	255.255.255.0
	Em1	172.16.30.26	255.255.255.252
PLANTEL 8	**Em0**	172.16.8.254	255.255.255.0
	Em1	172.16.30.30	255.255.255.252
PLANTEL 9	**Em0**	172.16.9.254	255.255.255.0
	Em1	172.16.30.34	255.255.255.252
PLANTEL 10	**Em0**	172.16.10.254	255.255.255.0
	Em1	172.16.30.38	255.255.255.252
PLANTEL 11	**Em0**	172.16.11.254	255.255.255.0
	Em1	172.16.30.42	255.255.255.252
PLANTEL 12	**Em0**	172.16.12.254	255.255.255.0
	Em1	172.16.30.46	255.255.255.252
PLANTEL 13	**Em0**	172.16.13.254	255.255.255.0
	Em1	172.16.30.50	255.255.255.252
PLANTEL 14	**Em0**	172.16.14.254	255.255.255.0
	Em1	172.16.30.54	255.255.255.252
PLANTEL 15	**Em0**	172.16.15.254	255.255.255.0
	Em1	172.16.30.58	255.255.255.252
PLANTEL 16	**Em0**	172.16.16.254	255.255.255.0
	Em1	172.16.30.62	255.255.255.252
PLANTEL 17	**Em0**	172.16.17.254	255.255.255.0
	Em1	172.16.30.66	255.255.255.252
PLANTEL 18	**Em0**	172.16.18.254	255.255.255.0
	Em1	172.16.30.70	255.255.255.252
PLANTEL 19	**Em0**	172.16.19.254	255.255.255.0
	Em1	172.16.30.74	255.255.255.252
PLANTEL 20	**Em0**	172.16.20.254	255.255.255.0
	Em1	172.16.30.78	255.255.255.252

De esta manera, la asignación de direcciones es la siguiente en cada una de las interfaces de los dispositivos entre planteles.

Al configurar la dirección IP de la subinterfaz correspondiente en el Router-on-a-stick como la dirección de la salida predeterminada, se agrega una ruta por defecto que enviará los paquetes generados en la red LAN con dirección a cualquier destino de Internet a la salida, este se encargará de reenviarlos a través de la red interna del IEMS hasta Internet.

En cada una de las redes locales de los planteles, los equipos de los administradores de red, los directivos, el personal administrativo y de confianza, dispositivos de los profesores y también los equipos dedicados, tal es el caso de teléfonos e impresoras, tendrán que recibir una dirección IP que será asignada al equipo a través de su dirección MAC. De esta manera se ha controlado que el equipo de cómputo del usuario obtenga la dirección IP que le corresponde y así tener control del direccionamiento.

2.4.1 Configuración de DHCP a través de las direcciones MAC en PfSense

En varias ocasiones es necesario tener algunas direcciones IP del espacio de direccionamiento de una red local para uso exclusivo de ciertos dispositivos, ya sea porque son servidores, impresoras, teléfonos IP, e incluso equipos de cómputo de algunos usuarios que necesitan ser diferenciados para ofrecerles cierto tipo de servicio. A continuación se tratará la forma en que se configura el equipo PfSense para que las direcciones IP que DHCP se asignen por medio de la dirección física.

Una de las formas para asignar una dirección IP estática sería configurando en cada equipo su dirección IP de manera manual y modificar en el rango de direcciones IP que se asignan dinámicamente; sin embargo, podría ocurrir en caso en el que el usuario no esté geográficamente cerca para que se realice la tarea por lo que se optará utilizar una característica del servicio de DHCP en PfSense en la que se determina que ciertas direcciones IP se asignen a equipos a través de su dirección física (su dirección MAC). Figura 2.9.

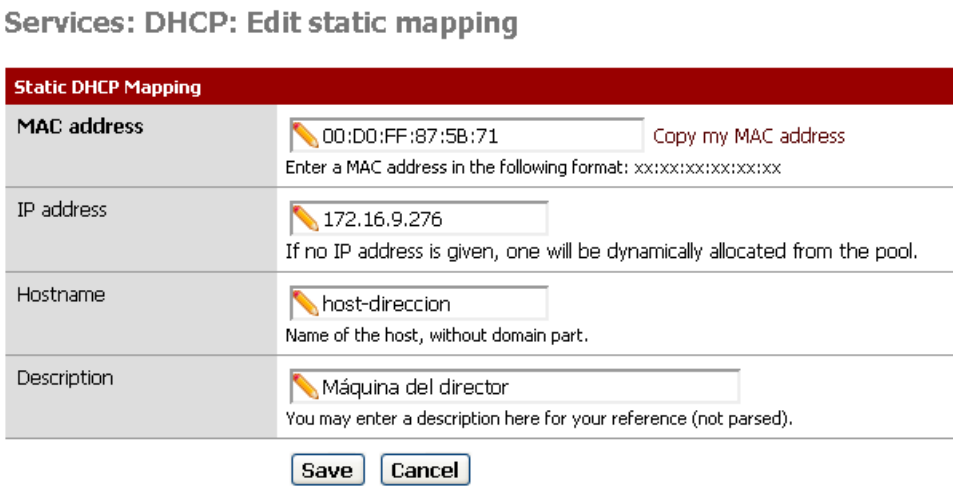

Figura 2.37. Configuración de DHCP para asignación de IP a través de MAC

Para realizar esta tarea es necesario contar con las direcciones físicas de los dispositivos a los que se les asignará un direccionamiento propio. Esta configuración se ejecutará en la interfaz web del dispositivo (WebConfigurator de PfSense) ingresando en la sección *Services*, opción *DHCP Server*. Se abrirá una vista en la que aparecen las interfaces que se encuentran en el dispositivo, se deberá elegir la interfaz de la LAN. Se despliega la configuración para DHCP que se utiliza en ese momento, es decir, dirección IP de la interfaz LAN, máscara de subred y rango de asignación dinámica principalmente. Debajo de esa información se encuentra una tabla en la que se especifican las direcciones IP que serán asignadas a través de la dirección MAC. Sin embargo, si nunca se ha realizado dicha configuración, la tabla aparecerá vacía. Si se desea agregar una entrada a esa tabla, se hace por medio del botón "+", hecho lo anterior se despliega una pantalla en la que se ingresa la dirección física del equipo al que se le asignará direccionamiento, la dirección IP que se asignará, el nombre del equipo (este valor, así como la dirección física del equipo se obtiene por medio del comando *ipconfig /all* en Windows o *uname –a* e *ifconfig* para Unix/Linux).

En la figura anterior se muestra un ejemplo de la manera en que se ingresaría la información al mapeo estático de DHCP para que el equipo con la dirección MAC dada tome la dirección IP determinada. Este tipo de acciones son necesarias cuando se requieren grupos definidos de usuarios que tienen necesidades en común. Este tipo de configuraciones son necesarias cuando se requieren aplicar ciertos permisos de acceso en algunos equipos de la red local, por ejemplo, perfiles para el servidor proxy.

Cuando le equipo con dicha dirección MAC se integre a la red local y solicite una dirección IP, el servidor realizará su asignación basándose en la dirección física. La información como DNS, dirección del la puerta de enlace predeterminada y nombre del dominio serán los mismos que los que se envían a través del rango normal de direcciones para DHCP.

2.5 Configuración de VLAN

El direccionamiento entre cada uno de los Routers de los planteles con el Router que enlaza con Internet y las redes de las oficinas centrales se hará por medio de VLAN. ¿Por qué el uso de VLAN en los enlaces WAN? Sin el uso de redes VLAN, cada uno de los planteles se tiene que conectar por medio de un enlace físico a una interfaz del Router que redireccionará el tráfico hacía Internet. De esta manera, el Router debe de tener 20 interfaces para poder dar servicio a todos los planteles además de una Interfaz que enlazará con las redes externas. Esto no es muy conveniente en la organización física de los dispositivos, además de que los Routers no están diseñados para tener un gran número de interfaces de red.

Para enlazar a todos los planteles en un solo punto, se hace necesario contar con un Router que esté equipado con una interfaz con la capacidad apta para soportar la cantidad de tráfico generado por las diversas subredes. Esta interfaz estará conectada a un Switch, dispositivo que por su naturaleza, tiene gran número de interfaces, las suficientes para interconectar a todos los planteles. En la infraestructura del IEMS, esté será un Switch de alta velocidad. La interfaz de interconexión en el Router de enlace se dividirá en subinterfaces, cada una de ellas asociada a una VLAN, misma que estará definida por el proveedor de los enlaces L2L. Cada plantel se configurará con la dirección IP correspondiente que haya resultado del cálculo del direccionamiento. El Router separa el tráfico de los planteles gracias a las VLAN.

Como ya se mencionó anteriormente, los identificadores (ID) para las VLAN han sido proporcionados por el proveedor de los enlaces L2L, es decir, cada uno de los equipos configurados en la red se le asignará el ID de la VLAN del enlace extendido correspondiente. Esta es la asignación de los identificadores para cada plantel según el enlace extendido que le conectará. A continuación se presenta la asignación de los identificadores utilizado como ejemplo para la muestra de la puesta en ejecución dentro de este documento:

- VLAN 10 para el enlace con el Router del plantel 1.
- VLAN 20 para el enlace con el Router del plantel 2.
- VLAN 30 para el enlace con el Router del plantel 3.
- VLAN 40 para el enlace con el Router del plantel 4.
- VLAN 50 para el enlace con el Router del plantel 5.
- VLAN 60 para el enlace con el Router del plantel 6.
- VLAN 70 para el enlace con el Router del plantel 7.
- VLAN 80 para el enlace con el Router del plantel 8.
- VLAN 90 para el enlace con el Router del plantel 9
- VLAN 100 para el enlace con el Router del plantel 10.
- VLAN 110 para el enlace con el Router del plantel 11.
- VLAN 120 para el enlace con el Router del plantel 12.
- VLAN 130 para el enlace con el Router del plantel 13.
- VLAN 140 para el enlace con el Router del plantel 14.
- VLAN 150 para el enlace con el Router del plantel 15.

- VLAN 160 para el enlace con el Router del plantel 16.
- VLAN 170 para el enlace con el Router del plantel 17.
- VLAN 180 para el enlace con el Router del plantel 18.
- VLAN 190 para el enlace con el Router del plantel 19.
- VLAN 200 para el enlace con el Router del plantel 20.

Cada una de las interfaces del Switch de enlace estará asignada a una VLAN diferente. La configuración de cada uno de los enlaces estará hecha como modo de acceso (tráfico de datos) que recibirá uno de los extremos de los enlaces LAN-to-LAN de los planteles. Figura 2.10.

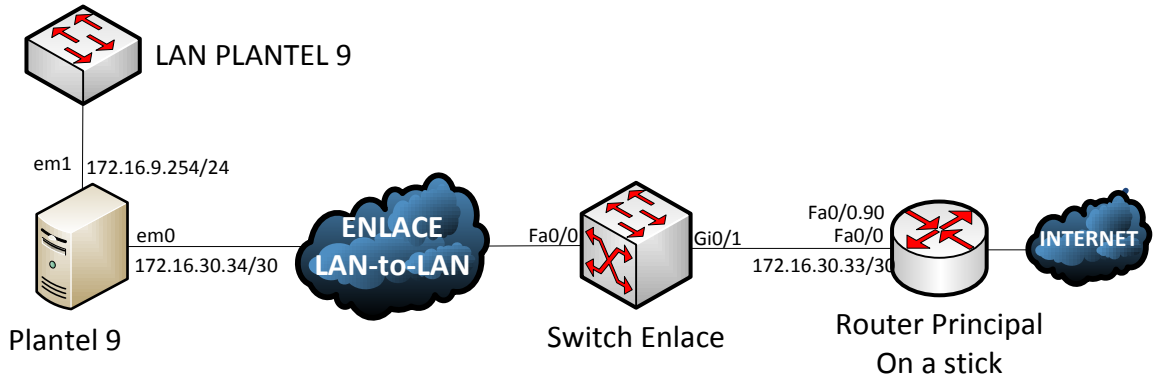

Figura 1.38. Conexión entre plantel y Switch de a través de enlace L2L

El procedimiento que se mostrará a continuación para la configuración del Switch no es el mismo que se utiliza para la configuración del Switch del proveedor, sin embargo, esta es la manera como se implementaría en el caso de que el proveedor sólo proporcionará los enlaces sin el Switch. Este ejemplo de configuración es la ejecutada en cualquier Switch de la marca Cisco®:

- Creación de las VLAN en el Switch.

```
Switch-Enlace(config)#vlan 10
Switch-Enlace(config-vlan)#name Plantel-1
Switch-Enlace(config-vlan)#vlan 20
Switch-Enlace(config-vlan)#name Plantel-2
Switch-Enlace(config-vlan)#
.
.
.
Switch-Enlace(config-vlan)#vlan 200
Switch-Enlace(config-vlan)#name Plantel-9
```

Los comandos anteriores sólo realizan la creación de las VLAN en el dispositivo y agregan una descripción a la interfaz acerca de su funcionamiento. La descripción se asocia al plantel que generará datos para dicha red VLAN.

- Asignación de puertos a las VLAN

```
interface FastEthernet0/1
description ENLACE AL PLANTEL 1
```

```
switchport access vlan 10
switchport mode access

interface FastEthernet0/2
description ENLACE AL PLANTEL 2
switchport access vlan 20
switchport mode access
.
.
interface FastEthernet0/20
description ENLACE AL PLANTEL 20
switchport access vlan 200
switchport mode access
```

La configuración de la interfaz está dedicada a cada uno de los planteles como un puerto en modo de acceso (tráfico de datos) para la VLAN específica a cada plantel. De esta manera se está separando el tráfico creando 20 dominios de broadcast independientes gracias a las propiedades de las VLAN.

Este Switch de alta velocidad tiene una interfaz dirigida al Router que permitirá la salida a Internet, tal como se puede ver en la figura 2.11. Este puerto debe ser configurado como troncal, ya que a través de él circularán los datos de todos los planteles, cada uno encapsulará en una VLAN distinta los datos que se generen dentro de ellas; sin embargo, se asignará a una *VLAN nativa* a la que se enrutará el tráfico que no pertenezca a ninguna VLAN (tráfico no etiquetado), esta VLAN será la 99 que sustituirá a la VLAN 1 que está dada por defecto en el dispositivo. La configuración de aquella interfaz es la siguiente:

```
interface GigabitEthernet0/1
switchport trunk native vlan 99
switchport trunk encapsulation dot1q
switchport mode trunk
```

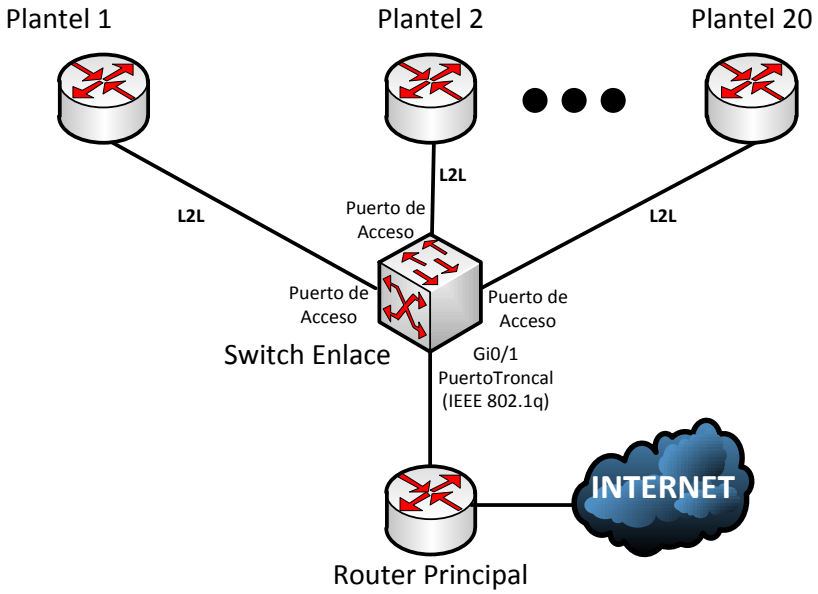

Figura 2.39. Puertos de acceso y enlace troncal.

De esta manera se tiene la conexión de los planteles a través de una red WAN sobre una red dividida en subredes y conectadas al Router principal a través de subinterfaces; sin embargo, cada uno de los enlaces es independiente el uno del otro sin comunicación entre sí. Para permitir el ruteo entre los enlaces de los planteles, se configurará el Router de enlace a Internet como Router-on-a-stick.

2.6 Configuración del ruteo: ruteo entre VLAN (Router-on-a-stick) y ruteo hacia Internet

En esta sección se presentará el esquema de ruteo que se propone en la red que se ha estado planteando. No se tratará sobre algún protocolo de enrutamiento dinámico, este se explicará en el proceso de mejora.

La configuración del ruteo entre las VLAN es posible a través de un Router. Este dispositivo será el mismo que enrutará el tráfico de las redes locales de cada plantel hacía Internet. El ruteo entre VLAN es necesario para mantener comunicados a todos los planteles, estos se podrían mantener aislados, pero no se conseguirían compartir recursos, aplicaciones ni información entre si directamente.

El Router enlazará a todos los planteles a través de una de sus interfaces. Esta interfaz será dividida en interfaces virtuales (subinterfaces), una correspondiente para cada plantel. Por esta razón, cada subinterfaz estará configurada para recibir tráfico de una VLAN utilizando IEEE 802.1q.

Tabla 2.6. Direccionamiento para las subinterfaces

Dispositivo	Interfaz	Dirección IP	Máscara de subred
ROUTER PRINCIPAL	**Fa0/0.10**	172.16.30.1	255.255.255.252
	Fa0/0.20	172.16.30.5	255.255.255.252
	Fa0/0.30	172.16.30.9	255.255.255.252
	Fa0/0.40	172.16.30.13	255.255.255.252
	Fa0/0.50	172.16.30.17	255.255.255.252
	Fa0/0.60	172.16.30.21	255.255.255.252
	Fa0/0.70	172.16.30.25	255.255.255.252
	Fa0/0.80	172.16.30.29	255.255.255.252
	Fa0/0.90	172.16.30.33	255.255.255.252
	Fa0/0.100	172.16.30.37	255.255.255.252
	Fa0/0.110	172.16.30.41	255.255.255.252
	Fa0/0.120	172.16.30.45	255.255.255.252
	Fa0/0.130	172.16.30.49	255.255.255.252
	Fa0/0.140	172.16.30.53	255.255.255.252
	Fa0/0.150	172.16.30.57	255.255.255.252
	Fa0/0.160	172.16.30.61	255.255.255.252
	Fa0/0.170	172.16.30.65	255.255.255.252
	Fa0/0.180	172.16.30.69	255.255.255.252
	Fa0/0.190	172.16.30.73	255.255.255.252
	Fa0/0.200	172.16.30.77	255.255.255.252

A continuación se muestra la configuración de las subinterfaces de un Router de marca Cisco®, ejemplificando las primeras tres subinterfaces que enlazan a los equipos del *Plantel 1*, *Plantel 2* y *Plantel 3* correspondientes a los enlaces WAN en las VLAN 10, 20 y 30. Es importante recordar que estos identificadores de VLAN son de ejemplo, los proporcionados por el proveedor para el transporte de datos entre los planteles son otros. La configuración puede cambiar según la versión de sistema operativo sobre la que esté trabajando el dispositivo, la esencia es la misma:

```
interface FastEthernet0/0  ! Se habilita
no ip address              ! La interfaz física no requiere dirección IP
no shutdown                ! Es importante que la interfaz física esté activada

interface FastEthernet0/0.10      ! Subinterfaz 10
encapsulation dot1Q 10            ! Se etiqueta sobre la VLAN 10
ip address 172.16.30.1 255.255.255.252

interface FastEthernet0/0.20
encapsulation dot1Q 20
ip address 172.16.30.5 255.255.255.252

interface FastEthernet0/0.30
encapsulation dot1Q 30
ip address 172.16.30.9 255.255.255.252
```

La interfaz FastEthernet 0/0 está conectada directamente al Switch y tiene que estar activada, no requiere de una dirección IP. La configuración de las subinterfaces se realiza colocando el nombre de la interfaz seguida de un punto y el número que identifica a la VLAN que va a enrutar (se hace esto para identificar la VLAN que enrutará la interfaz, no tiene impacto en el funcionamiento), por ejemplo, la subinterfaz*FastEthernet0/0.20* que enrutará por medio del estándar dot1Q (**IEEE 802.1q**) a la VLAN 20. Cada una de las subinterfaces utilizará una de las direcciones correspondientes al espacio de direccionamiento calculado anteriormente para los enlaces WAN con direcciones de máscara 255.255.255.252.

La interfaz FastEthernet0/0 del Router está conectado *al Switch de enlace de alta velocidad* a través de un enlace troncal que está asignada a la VLAN 99 como nativa, así que por esta razón se tiene que crear la subinterfaz que redireccione el tráfico dirigido a la VLAN 99, tal es el caso del tráfico no etiquetado (que no pertenece a ninguna VLAN).

```
interface FastEthernet0/0.99
encapsulation dot1Q 99 native
```

Cada uno de los Router pfSense en los planteles debe de tener configurada su dirección IP de salida, dirigida hacia el enlace en el Router on a stick. De esta manera, los dispositivos podrán enviar los paquetes generados a diferentes redes fuera de sus redes LAN.

Por ejemplo, el resultado del cálculo del direccionamiento determina que para el enlace WAN del Router del Plantel 9 la dirección de red 172.16.30.32 con máscara 255.255.255.252, la dirección más baja es asignada a la subinterfaz del Router-on-a-stick mientras que la más alta al Router pfSense del plantel. Por esta razón, la dirección 172.16.30.33 es la dirección de salida del Router del plantel.

La dirección de salida en todos los Routers debe de ser configurado para tener comunicación entre los enlaces WAN. La comprobación de la comunicación puede ser realizada por medio del comando ping desde el Router del Plantel 9 al Router del plantel 1 con la dirección IP en su interfaz WAN 172.16.30.2, figura 2.12.

```
Enter an option: 7


Enter a host name or IP address: 172.16.30.2

PING 172.16.30.2 (172.16.30.2): 56 data bytes
64 bytes from 172.16.30.2: icmp_seq=0 ttl=64 time=47.378 ms
64 bytes from 172.16.30.2: icmp_seq=1 ttl=64 time=0.203 ms
64 bytes from 172.16.30.2: icmp_seq=2 ttl=64 time=0.201 ms

--- 172.16.30.2 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.201/15.927/47.378/22.239 ms

Press ENTER to continue.
```

Figura 2.40. Ping desde el Plantel 9 a Plantel 1

Se puede verificar la comunicación con el Router del plantel 2 que tiene la dirección 172.16.30.6 configurada en su interfaz WAN., figura 2.13.

```
Enter an option: 7


Enter a host name or IP address: 172.16.30.6

PING 172.16.30.6 (172.16.30.6): 56 data bytes
64 bytes from 172.16.30.6: icmp_seq=0 ttl=64 time=7.730 ms
64 bytes from 172.16.30.6: icmp_seq=1 ttl=64 time=2.751 ms
64 bytes from 172.16.30.6: icmp_seq=2 ttl=64 time=2.412 ms

--- 172.16.30.6 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 2.412/4.298/7.730/2.431 ms

Press ENTER to continue.
```

Figura 2.413 Comunicación entre Plantel 9 y Plantel 2

De esta manera, todos los planteles se comunican entre sí, las redes LAN en cada uno de los Routers pfSense puede comunicarse a través de un ping a las interfaces del Routers de cualquier otro plantel, el ruteo entre VLAN está funcionando.

En lo que respecta a la salida hacia Internet, el Router on a stick que tiene conectados a todos los planteles a través de subinterfaces tiene una ruta predeterminada al dispositivo que le da salida a Internet, en este caso un equipo sobre OpenBSD. Para mostrar la configuración del ruteo de los dispositivos, se muestra el siguiente diagrama con un direccionamiento propuesto establecido en las interfaces de los dispositivos.

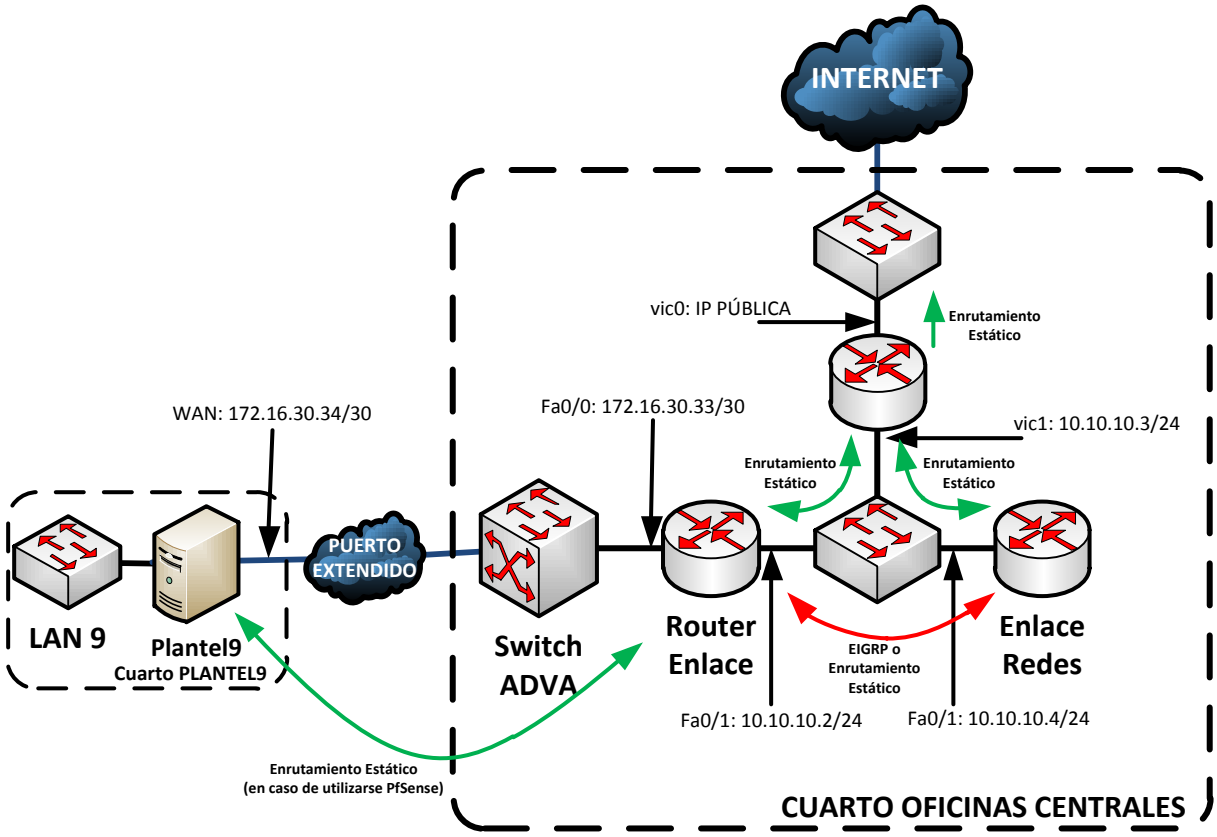

Figura 2.42. Planteamiento del esquema de ruteo con Routers PfSense en los planteles.

En la figura 2.14 se presenta el esquema de ruteo en el que se tiene Routers bajo PfSense en la salida de los planteles. Estos equipos no permiten un ruteo dinámico, pero se pueden configurar un esquema estático. En el Router PfSense se mostró la configuración de la dirección de salida en su interfaz gráfica llamada "WebConfigurator", sin embargo, a través de la Interfaz de Línea de Comandos la configuración se muestra a continuación, siguiendo el direccionamiento mostrado en la figura:

```
route add default 172.16.30.33
```

En el Router on stick (nombrado en la figura Router Enlace debido a que "enlaza" a todos los planteles) la configuración de la ruta predeterminada para salir hacia el enlace a Internet es la siguiente:

```
ROUTER(config)#ip route 0.0.0.0 0.0.0.0 FastEthernet 0/1 10.10.10.3
ROUTER(config)#end
ROUTER#show running-config | include ip route 0.0.0.0
ip route 0.0.0.0 0.0.0.0 FastEthernet0/1 10.10.10.3
ROUTER#
```

Esta ruta estática en el Router indica que se alcanzará a cualquier ruta que no esté en la tabla de ruteo a través de la Interfaz FastEthernet 0/1 (que es la salida natural al exterior que tiene este dispositivo), su siguiente salto es la dirección IP de su Router de salida, en este caso particular, el Router OpenBSD tiene la dirección IP 10.10.10.3 en su interfaz *vic1*, la segunda interfaz nombrada *vic0* es la que se encuentra conectada al enlace hacia internet con el proveedor de servicio.

El Router llamado “Enlace Redes” es el encargado de dar salida a las redes de las oficinas centrales de la Institución educativa.

Si bien, ya se tiene configurado el ruteo entre VLAN, la comunicación que se ha logrado es entre los Routers de cada plantel, no así entre redes locales, por eso es necesaria la configuración de una ruta estática para cada una de las redes locales en el Router On a Stick, esa configuración es la siguiente:

```
ip route 172.16.1.0 255.255.255.0 FastEthernet0/0.10 172.16.30.2
ip route 172.16.2.0 255.255.255.0 FastEthernet0/0.20 172.16.30.6
ip route 172.16.3.0 255.255.255.0 FastEthernet0/0.30 172.16.30.10
ip route 172.16.4.0 255.255.255.0 FastEthernet0/0.40 172.16.30.14
ip route 172.16.5.0 255.255.255.0 FastEthernet0/0.50 172.16.30.18
ip route 172.16.6.0 255.255.255.0 FastEthernet0/0.60 172.16.30.22
ip route 172.16.7.0 255.255.255.0 FastEthernet0/0.70 172.16.30.26
ip route 172.16.8.0 255.255.255.0 FastEthernet0/0.80 172.16.30.30
ip route 172.16.9.0 255.255.255.0 FastEthernet0/0.90 172.16.30.34
ip route 172.16.10.0 255.255.255.0 FastEthernet0/0.100 172.16.30.38
ip route 172.16.11.0 255.255.255.0 FastEthernet0/0.110 172.16.30.42
ip route 172.16.12.0 255.255.255.0 FastEthernet0/0.120 172.16.30.46
ip route 172.16.13.0 255.255.255.0 FastEthernet0/0.130 172.16.30.50
ip route 172.16.14.0 255.255.255.0 FastEthernet0/0.140 172.16.30.54
ip route 172.16.15.0 255.255.255.0 FastEthernet0/0.150 172.16.30.58
ip route 172.16.16.0 255.255.255.0 FastEthernet0/0.160 172.16.30.62
ip route 172.16.17.0 255.255.255.0 FastEthernet0/0.170 172.16.30.66
ip route 172.16.18.0 255.255.255.0 FastEthernet0/0.180 172.16.30.70
ip route 172.16.19.0 255.255.255.0 FastEthernet0/0.190 172.16.30.74
ip route 172.16.20.0 255.255.255.0 FastEthernet0/0.200 172.16.30.78
```

En lo que se refiere a la configuración del ruteo en el Router PfSense que da salida a toda la Institución, con una simple ruta predeterminada al enlace de Internet del proveedor se tiene acceso a Internet. Esta configuración es realmente sencilla por parte de la Institución, la configuración del lado del proveedor de servicios no es relevante para el funcionamiento de la red local.

Para que el Router OpenBSD llegue a las redes locales, es necesario configurar las rutas estáticas correspondientes. Para el esquema de direccionamiento propuesto, las redes de los planteles se encuentra en el espacio de direccionamiento de un segmento de red de clase B 172.16.0.0/16, mientras que las redes de las oficinas centrales son los segmentos de clase C 192.168.1.0/24, 192.168.3.0/24 y 192.168.3.0/2. La configuración de las rutas estáticas es la siguiente:

```
route add -net 172.16.0.0/16 10.10.10.2
route add -net 192.16.0.0/16 10.10.10.3
```

En ambas rutas estáticas se utiliza el criterio en la que se utiliza la dirección del siguiente salto. En la primera ruta estática mostrada, esta apunta al segmento con clase y utiliza el criterio de la dirección IP del siguiente salto, es decir, la dirección IP de la interfaz FastEthernet 0/1 del Router on a stick que utiliza como su salida. La ruta estática apunta a la superred 192.16.0.0 que incluye a las redes de las oficinas centrales.

Por otra parte, la interfaz del equipo OpenBSD que está conectada a Internet debe de estar configurada con una dirección IP pública que debió haber sido provista por el proveedor de servicios. Esta dirección IP es la que se utilizará para comunicar a la red local con Internet. Para hacer posible esto, es necesario aplicar NAT en la interfaz vic0 del Router OpenBSD. Se deben crear las reglas de filtrado correspondiente en el archivo */etc/pf.conf* de la siguiente manera y aplicar el filtrado para que tenga efecto. En el próximo capítulo se tratará de manera más

profunda la instalación y configuración de OpenBSD para que este sistema funcione como un Router/Firewall, en esta sección del documento se tratarán los puntos básicos para que OpenBSD reenvíe paquetes sin ningún tipo de filtrado.

```
EXT="vic0"
INT="vic1"
RED="{ 172.16.0.0/16 192.168.0.0/16 }"
pass in on $INT from $RED
match out quick on $EXT from $RED to any nat-to $EXT
pass out quick on $EXT from any to any
```

Este archivo de configuración de /etc/pf.conf utiliza macros para las interfaces del equipo. La macro EXT (por exterior) hace referencia a la interfaz vic0 que conecta al equipo con el enlace de Internet. La macro INT (por interior) hace referencia a la interfaz vic1 que conecta al equipo con la red privada de la Institución. La macro RED tiene a los dos segmentos de red utilizados de la institución, la red de clase B de los planteles, y la superred de las oficinas centrales.

La primera regla indica que se dejará pasar el tráfico proveniente de las redes locales *pass in on $INT from $RED*. La segunda regla, *match out quick on $EXT from $RED to any nat-to $EXT* señala que el tráfico proveniente de las redes locales que salga a través de la interfaz externa sea trasladado a la dirección IP de la interfaz externa, es decir, a la IP pública. La última regla, *pass out quick on $EXT from any to any* señala al filtro de paquetes que se dejará pasar todo el tráfico generado que salga a través de la interfaz de salida, no hay restricción alguna.

Para que las reglas tengan efecto, la variable *net.inet.ip.forwarding* del del archivo */etc/sysctl.conf* tiene que estar en 1, si no es así, se debe de modificar para que así sea y reiniciar el equipo. Para aplicar las reglas del filtro de paquetes se ejecuta el comando *pfctl –f /etc/pf.conf*.

De esta manera se tiene configurado el ruteo de la red de una manera estática. Una gran ventaja de tener este esquema de direccionamiento radica en los Routers, cuando se tiene que enrutar un paquete hacia una red específica, las rutas estáticas ofrecen rapidez en el ruteo ya que el dispositivo no tiene que realizar ningún cálculo para buscar la mejor ruta, ya está establecida. Sin embargo, en caso de fallas o migración de direccionamiento, la tabla de ruteo es estática y se tiene que generar de nueva cuenta.

2.7 Procesos de mejora continua en la infraestructura de red

La red que se ha propuesto en este trabajo tiene en cada uno de los planteles un Router que direcciona el tráfico generado en la red LAN hacia el resto de la red a Internet. Este Router es un equipo de cómputo con el sistema operativo pfSense instalado con la funcionalidad de reenvío de paquetes, lo cual permite al dispositivo realizar dicha tarea. La elección de utilizar equipos de cómputo produce que los costos por la implementación de un Router sean de menor costo. Sin embargo, es necesario contemplar la sustitución de los Router pfSense por uno de una marca conocida, como CISCO®, que brindan la funcionalidad requerida y de seguridad, además, no se requiere ningún cambio en la infraestructura de red con respecto al tipo de medio de transmisión a utilizar, las interfaces que están integradas permiten la conexión de la red LAN y del enlace L2L al dispositivo sin ningún problema.

Una de las principales ventajas que traería a la red de datos la implementación de una red sobre Routers de algún distribuidor de dispositivos de red es la implementación de protocolos de ruteo dinámico, que ofrecen rápida convergencia de la red, y un menor índice de accesos a los dispositivos de red para cambios de configuración, pues no es necesario cambiar la tabla de ruteo de manera manual, el protocolo de ruteo lo realiza de manera automática.

Se propone que se utilice Cisco® porque es una empresa líder en abasteciendo dispositivos de red a varias compañías, desde Proveedores de Servicios de Internet, hasta pequeñas y medianas redes de datos. Ofrecen servicio

de soporte en caso de fallas en los dispositivos con personal calificado que se ubica en cualquier lugar del mundo. La documentación de cualquier dispositivo es fácil de encontrar en su sitio web para cualquiera de sus equipos, tipo de configuración o problema presentado. Además, una interacción con la empresa multinacional, conjuntamente de los beneficios otorgados a través de los contratos comerciales, se puede crear una interacción académica para el desarrollo de personal calificado en conocimientos desde básicos a avanzados en telecomunicaciones. Por tal motivo, las configuraciones que se expondrán a continuación se basarán en los comandos aceptados por un Router Cisco® 2911 sobre sistema operativo Cisco IOS, versión 15.3.

A continuación se mostrará la configuración del Router en el Plantel 9 como se trató anteriormente durante la configuración del Router pfSense del mismo plantel.

La configuración del dispositivo que conecta a la red del Plantel 9 es la siguiente: De la red 172.16.9.0/24 se tomará la dirección más alta en el rango de direcciones (172.16.9.254); esta es la dirección de salida de la red y se configurará en la interfaz FastEthernet 0/1 del Router ya que esta conecta a la su LAN. La dirección de red que conecta al enrutador con la red WAN será la última del rango de 172.16.30.34/30 en la interfaz FastEthernet 0/0.

Interfaz	Dirección de red	Función
LAN	172.16.9.254/24	Salida de la red local.
WAN	172.16.30.34/30	Conexión con el Router de Enlace

Tabla 2.7. Asignación de direccionamiento en el equipo del plantel 9

La configuración es la siguiente[4]:

```
interface FastEthernet0/0
description ENLACE WAN PLANTEL 9
ip address 172.16.30.34 255.255.255.252

Interface FastEthernet0/1
description LAN PLANTEL 9
ip address 172.16.9.254 255.255.255.0
```

Para el servicio de DHCP en la red local se configura un pool de direccionamiento para el servicio. Este indicará el rango de direcciones de la red local disponible. Asimismo, se presenta la configuración para la asignación de direccionamiento estático por medio de dirección MAC que también se implementó en los Routers PfSense. Por añadidura se presenta la configuración del pool de DHCP dinámico y el estático para una impresora y para la red local.

```
ip dhcp pool IMPRESORA_1
 host 172.16.9.225 mask 255.255.255.0
 hardware-address 00E0.B017.9162 ieee802
 client-name IMPRESORA_1
 default-router 172.16.9.254
 domain-name plantel9.iems.edu.mx
 dns-server <Dirección-IP-DNS-locales-o-remotos>
```

[4]Las configuraciones para los routers mostradas en este documento son para un Router CISCO® modelo 2911 ejecutando el sistema operativo Cisco IOS versión 15.3.

```
ip dhcp pool DHCP_LOCAL
 network 172.16.9.0 255.255.255.0
 default-router 172.16.9.254
 domain-name plantel9.iems.edu.mx
 dns-server <Dirección-IP-DNS-locales-o-remotos>
```

En la configuración anterior se presentaron los comandos a utilizar para los equipos de la red local, así como para un equipo dentro de la LAN pero que se requiere determinada dirección IP sea de dicho equipo. Todos los equipos de directivos, administrativos y personal de confianza, así como de dispositivos dedicados como teléfonos e impresoras, se tendrá que realizar dicha configuración para que la dirección IP que obtengan esté determinada por su dirección MAC.

En otro tema, para cada uno de los Routers es necesaria la configuración de la ruta estática por defecto por medio de una ruta estática a la dirección ubicada en el Router on a stick.

La configuración de la ruta estática es la siguiente:

```
Plantel-9(config)# ip route 0.0.0.0 0.0.0.0 FastEthernet0/0 172.16.30.33
```

La dirección de salida en todos los Router debe de ser configurada para tener comunicación entre los enlaces WAN. La comprobación de la comunicación puede ser realizada por medio del comando ping desde el Router del Plantel 9 al Router del plantel 1 con la dirección IP en su interfaz WAN 172.16.30.2.

```
Plantel-9#ping 172.16.30.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.30.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/71/94 ms

Plantel-9#
```

Se puede verificar de la misma forma la comunicación con el Router del plantel 2, esto gracias al ruteo entre VLAN que realiza el Router on a stick:

```
Plantel-9#ping 172.16.30.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.30.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 37/69/111 ms

Plantel-9#
```

Sin embargo, si se desea tener comunicación entre las redes LAN de los planteles, no se efectuará debido a que la tabla de ruteo de cada plantel sólo cuenta con las entradas correspondientes a las redes conectadas directamente a sus interfaces y la ruta estática configurada. Cuando se realice el envío de paquetes a una red que no se encuentra en la tabla de ruteo, enviará el paquete fuera del Router gracias a la ruta predeterminada, sin embargo, el Router de salida no tiene ninguna entrada acerca de las redes de las LAN de cada plantel y se eliminará. A continuación se muestra la tabla de ruteo del Router configurado en el equipo Plantel 9:

```
Plantel-9#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.16.30.33 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       172.16.9.0/24 is directly connected, FastEthernet0/1
C       172.16.30.32/30 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 172.16.30.33, FastEthernet0/0
Plantel-9#
```

Las únicas dos redes alcanzables son la 172.16.9.0/24 y la red 172.16.30.320/30 que están conectadas directamente y están denotadas con la letra "C". La ruta estática predeterminada permitirá a este Router salir a través de su salida 172.16.30.33 que es el Router de salida.

La tabla de ruteo del Router Principal es la siguiente[5]:

```
ROUTER#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.12.1.180 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 24 subnets, 2 masks
C       172.16.30.0/30 is directly connected, FastEthernet0/0.10
C       172.16.30.4/30 is directly connected, FastEthernet0/0.20
C       172.16.30.8/30 is directly connected, FastEthernet0/0.30
C       172.16.30.12/30 is directly connected, FastEthernet0/0.40
C       172.16.30.16/30 is directly connected, FastEthernet0/0.50
C       172.16.30.20/30 is directly connected, FastEthernet0/0.60
C       172.16.30.24/30 is directly connected, FastEthernet0/0.70
C       172.16.30.28/30 is directly connected, FastEthernet0/0.80
C       172.16.30.32/30 is directly connected, FastEthernet0/0.90
C       172.16.30.36/30 is directly connected, FastEthernet0/0.100
C       172.16.30.40/30 is directly connected, FastEthernet0/0.110
C       172.16.30.44/30 is directly connected, FastEthernet0/0.120
C       172.16.30.48/30 is directly connected, FastEthernet0/0.130
C       172.16.30.52/30 is directly connected, FastEthernet0/0.140
C       172.16.30.56/30 is directly connected, FastEthernet0/0.150
C       172.16.30.60/30 is directly connected, FastEthernet0/0.160
C       172.16.30.64/30 is directly connected, FastEthernet0/0.170
C       172.16.30.68/30 is directly connected, FastEthernet0/0.180
C       172.16.30.72/30 is directly connected, FastEthernet0/0.190
C       172.16.30.76/30 is directly connected, FastEthernet0/0.200
ROUTER#
```

[5] En esta salida de comando se considera que las rutas estáticas que se configuraron anteriormente ya no están, el objetivo en esta sección del documento es la implementación de un protocolo de protocolo de enrutamiento dinámico.

La tabla de ruteo del Router Principal no tiene ninguna entrada a alguna de las redes locales de los planteles.

Actualmente, el esquema de red que se tiene con los Routers PfSense, el Router principal tiene configuradas rutas estáticas hacía las redes LAN de cada plantel, por ejemplo, la red local del plantel 1, la ruta estática se encuentra configurada de la siguiente manera:

```
ip route 172.16.1.0 255.255.255.0 FastEthernet0/0.10 172.16.30.2
```

El comando anterior especifica que se conocerá a la red 172.16.1.0/24 que pertenece al segmento de la red local del plantel 1 a través de la subinterfaz 10 de la interfaz física FastEthernet0/0, asimismo, la dirección IP 172.16.30.2 indica la dirección de siguiente salto del equipo, en este caso es la dirección IP de la interfaz WAN del Router PfSense del plantel 1. Esta forma en la que se configura una ruta estática brinda al equipo una forma sencilla de ruteo de paquetes a través de rutas estáticas, se indica al equipo la interfaz a la que se saldrá y la dirección del siguiente salto que se deben de utilizar para alcanzar la red destino, el equipo ya no hace ninguna búsqueda de la salida del paquete en el momento de reenviarlo. Sin embargo, esta forma de direccionamiento de paquetes se puede hacer tediosa cuando la red es amplia, y en caso de modificación a la red, se deben hacer bastantes cambios correspondientes a la configuración de ruteo estático. Por eso mismo, es recomendable la configuración de un protocolo de ruteo dinámico que ayude a la rápida y sencilla convergencia de la red en caso de algún cambio en la misma.

2.7.1 Implementación de protocolo de ruteo

Para lograr que todas las redes se comuniquen entre sí es necesario tener las tablas de ruteo con las entradas pertinentes que indiquen la ruta a cada una de las redes. El protocolo que se propone a utilizar junto con los Routers será Enhanced Interior Gateway Routing Protocol (Protocolo de Ruteo de Gateway Interior Mejorado, EIGRP) que es una mejora del protocolo IGRP. Ambos protocolos son propiedad de Cisco Systems®, y por tal hecho, sólo funcionan en Routers Cisco®. Cabe mencionar que el protocolo IGRP ya es obsoleto, en los sistemas operativos actuales de Cisco®, este protocolo ya no es posible de configurar.

2.7.1.1 El protocolo de ruteo EIGRP

El protocolo EIGRP es un protocolo Vector Distancia sin clase que ofrece mayores características que los demás protocolos Vector Distancia como RIPv1 y RIPv2. Esas características extras son las siguientes:

- Utilización del Protocolo de Transporte Confiable (*RTP, Reliable Transport Protocol*).

EIGRP fue diseñado para realizar el ruteo entre diversos protocolos como IP, IPX y AppleTalk, en la que estos dos últimos no pueden utilizar los servicios de UDP y TCP para el envío de paquetes. Debido a esto, EIGRP trabaja independiente de la capa de red del modelo TCP/IP y utiliza el Protocolo de Entrega Confiable sustituyendo a TCP ya que se requiere que el receptor de los mensajes envíe un acuse de recibo; sin embargo, puede realizar la entrega no confiable para realizar también tareas del protocolo UDP, los acuses de recibo no se realizan. Además, con la utilización de los Módulos Dependientes de Protocolo (PDM) se realizan las tareas correspondientes al protocolo utilizado, IP, IPX o AppleTalk.

Asimismo, es posible de realizar envíos unicast o multicast, esta última utilizando la dirección 224.0.0.10.

Los tipos de paquetes que utiliza EIGRP con RTP son:

- Paquete saludo: Por medio de entregas no confiables (sin acuse de recibo), el Router envía paquetes de saludo a todas sus interfaces para descubrir Routers vecinos y realizar adyacencias.

- Paquete de actualización: Se utilizan por los Routers para compartir información de ruteo. Esto se realiza cuando es necesario y sólo a los dispositivos que requieren de la información. Se realiza por medio de entregas confiables, los Routers que reciben una actualización envían un paquete de acuse de recibo (ACK). Las actualizaciones se envían como multicast cuando múltiples Routers requieren actualización[6], o unicast cuando sólo un Router es afectado por el cambio en la topología.
- Paquetes de consulta y respuesta: Estos paquetes utilizan RTP. Los paquetes consulta son enviados por multicast en busca de redes y otras tareas, mientras que los paquetes de respuesta son enviados por unicast ya que son respuesta a las consultas.

- Actualizaciones limitadas.

A diferencia de RIP, EIGRP no envía actualizaciones periódicas. En su lugar, EIGRP envía actualizaciones cuando la métrica de una ruta cambia. Las actualizaciones enviadas son *limitadas* debido a que no todos los Routers recibirán la actualización, sólo aquellos que se vean afectados. También, las actualizaciones serán parciales, sólo se enviarán los cambios realizados y no la información completa.

- Algoritmo de actualización por difusión (DUAL).

El algoritmo de actualización por difusión (DUAL) es utilizado para obtener la convergencia con EIGRP, a diferencia de otros protocolos que hacen uso de Bellman-Ford o Ford Fulkerson. El uso de DUAL permite que no se produzcan loops a lo largo del cálculo de una ruta. Permite que los Routers se sincronicen al mismo tiempo, y los Routers que no son afectados no participen en el recálculo. Para realizar los cálculos hace uso de una Máquina de estados finitos (FSM) que utiliza el valor de las métricas para obtener la ruta más eficiente sin loops de ruteo.

- Establecimiento de adyacencias.

Por medio de los mensajes de saludo, los Routers envían paquetes a los dispositivos vecinos para establecer comunicación y compartir información. Cuando un Router contesta un mensaje de saludo generándose una adyacencia. Envía a continuación un mensaje de consulta que es resuelta con la información de ruteo.

- Tablas de vecinos y topología

Después de haber establecido adyacencias con los demás Routers que manejan el mismo ID de proceso de ruteo de EIGRP, este aparece en la tabla de vecinos del Router y gracias al algoritmo DUAL cada Router tiene un mapa de la topología en su base interna de información.

La distancia administrativa en comparación con otros protocolos de Gateway interior es la menor. Cuando se configuran diversos protocolos de ruteo en un mismo Router de la marca Cisco®, este elegirá las rutas establecidas por medio de EIGRP. La distancia administrativa para rutas internas de 90, mientras que para rutas externas es de 170. Las rutas sumarizadas de EIGRP tienen una distancia administrativa 5.

Por otra parte, al igual que otros protocolos de ruteo, EIGRP puede implementar autenticación de sus actualizaciones de ruteo y demás mensajes generados.

A diferencia de RIP que utiliza como métrica los saltos (Routers) que se atravesaban a través de la red para llegar al destino, EIGRP utiliza un conjunto de valores que componen su métrica: Ancho de banda, retardo, confiabilidad y carga.

[6] Los envíos son multicast, es decir, no se envían a todos los Routers, pero si a un grupo numerosos de ellos que son afectados por algún cambio en la red y necesitan actualización.

El ancho de banda es la capacidad de transmisión de datos de la interfaz, que depende del medio que se esté utilizando, por default, cada interfaz de un Router Cisco® tiene configurado 1544 Kbits (valor de velocidad de un enlace E1). Es conveniente cambiar este valor por el verdadero según la capacidad de las interfaces quese están utilizando.

El retardo es el tiempo que le toma a los paquetes atravesar la ruta, el retardo configurado en las interfaces es de 2000 microsegundos que es el valor predeterminado para enlaces seriales (E1). Este valor ser puede modificar.

La confiabilidad es la posibilidad de que falle un enlace, un valor entre 0 y 1 que especifica este valor. Otro valor de métrica es la carga, cantidad de tráfico que utiliza un enlace. Estás dos métricas no se utilizan de manera predeterminada por EIGRP, sólo el valor del ancho de banda y retardo.

Actualmente Cisco está trabajando para volver a EIGRP un protocolo estándar y ayudar a las compañías que cuentan con una red *multivendor*[7] en el que la elección el administrador de red por algún protocolo de enrutamiento se base en méritos técnicos. Asimismo, está trabajando junto con la IETF para la liberación de un RFC con las especificaciones. Asimismo, la implementación de EIGRP como IGP de la red permite la implementación de IPv6, esto debido a que el protocolo fue diseñado para trabajar bajo esa versión de IP, cuestión que OSPF arregla en su versión 3.

2.7.1.2 Configuración de EIGRP

El protocolo EIGRP será implementado en la red institucional del IEMS porque ofrece mayores ventajas con respecto a los demás protocolos de ruteo, además de que la red está bajo una infraestructura de dispositivos Cisco®.

Para habilitar el protocolo de ruteo EIGRP en los Routers son necesarios los siguientes comandos en el modo de configuración global:

- **router eigrp** *número-de-sistema-autónomo:* Habilita el proceso de EIGRP en el Router. El número de sistema autónomo debe de ser el mismo en todos los Routers que participarán en el dominio de ruteo para poder compartir información.
- **network** *ip-red máscara-wildcard {opcional}:* Anuncia una red. La interfaz de red que coincida su dirección con la anunciada en el proceso de ruteo participará en el envío de actualizaciones de ruteo.
- **no auto-summary**: Evitar la sumarización automática. La sumarización automática de EIGRP generan rutas a la dirección de red con clase que generó alguna otra ruta con salida a una interfaz nula (***null interface***), por ejemplo, la red 172.16.10.128/25 genera la ruta a la red 172.16.0.0 con salida a la interfaz null0, si no hay coincidencia de un paquete que va a la red 172.16.10.0, la red a la interfaz nula si coincidirá, enviándose el paquete a la interfaz nula y perdiéndolo, sin tomar en cuenta la existencia de alguna ruta predeterminada.
- **passive-interface** *tipo-de-interfaz número-de-puerto*: este comando es útil para evitar que la interfaz especificada envíe actualizaciones EIGRP.

La configuración del proceso de EIGRP para toda la red del IEMS se identificará por el número de sistema autónomo (AS) 100. Este valor de AS no fue proporcionado por el proveedor de servicios (ISP), puede ser cualquier número. Este valor fue elegido para el ruteo dentro de la red WAN institucional.

La configuración del Plantel 1 para participar en el proceso de ruteo es la siguiente, así como la distribución de la configuración del direccionamiento se puede observar e la figura 2.15.

[7] Información que se puede encontrar en el sitio web
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6554/ps6599/ps6630/qa_C67-726299.html

```
Plantel-1(config)#router eigrp 100
Plantel-1(config-router)#network 172.16.30.0 0.0.0.3
Plantel-1(config-router)#network 172.16.1.0 0.0.0.255
Plantel-1(config-router)#passive-interface default
Plantel-1(config-router)#no passive-interface FastEthernet0/0
Plantel-1(config-router)#no auto-summary
Plantel-1(config-router)#
```

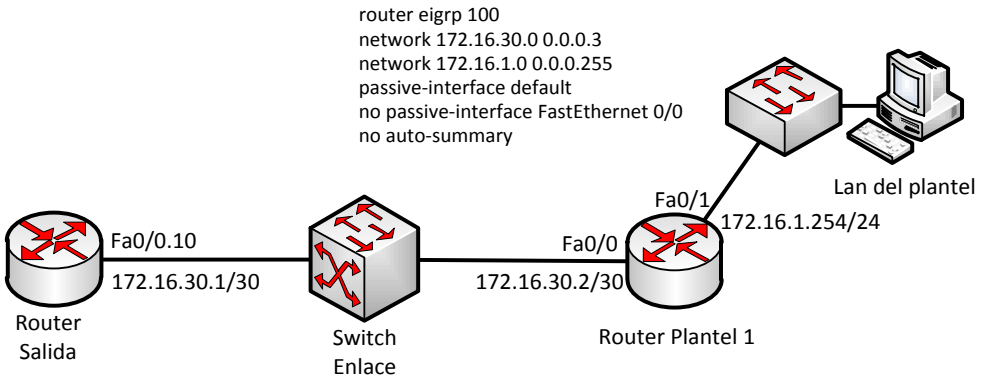

Figura 2.43. Configuración de EIGRP en el Router del Plantel 1

El comando ***router eigrp 100*** activa el proceso 100 de EIGRP en el Router, la línea ***network 172.16.30.0 0.0.0.3*** anuncia en el proceso de ruteo a la red 172.16.30.0 con máscara 255.255.255.252, el valor 0.0.0.3 es la máscara de Wildcard. La máscara de Wildcard informa al protocolo de ruteo que interfaces participarán en el proceso de EIGRP y así las redes a las que pertenecen las interfaces serán anunciadas. La máscara de Wildcard informa al protocolo de ruteo que la interfaz FastEthernet 0/0 participará en el proceso de ruteo, por lo que la red 172.16.30.0/30 será anunciada a los Routers vecinos.

Para garantizar que sólo se envían actualizaciones de ruteo en las interfaces necesarias, se utiliza el comando ***passive-interface default*** que inhabilita a todas las interfaces en el dispositivo para el envío de información de ruteo, sólo a través del comando ***no passive-interface interface [slot/puerto]*** se permite a la interfaz que se indica en el comando que esta podrá compartir actualizaciones. En los comandos mostrados arriba, la interfaz que no será pasiva y compartirá información de ruteo será la FastEthernet 0/0 que se conecta a los demás Routers a través del puerto L2L.

Todos los Routers de los planteles serán configurados de la misma forma, sólo cambian las direcciones en el argumento sobre el comando ***network***. A continuación se muestra la configuración del Router del plantel 20.

```
router eigrp 100
passive-interface default
no passive-interface FastEthernet0/0
network 172.16.30.76 0.0.0.3
network 172.16.20.0 0.0.0.255
no auto-summary
```

La configuración del Router de salida que enlaza todos los Routers se configura de la siguiente manera:

```
router eigrp 100
network 172.16.30.0 0.0.0.127
passive-interface default
no passive-interface FastEthernet0/0.10
no passive-interface FastEthernet0/0.20
no passive-interface FastEthernet0/0.30
no passive-interface FastEthernet0/0.40
no passive-interface FastEthernet0/0.50
no passive-interface FastEthernet0/0.60
no passive-interface FastEthernet0/0.70
no passive-interface FastEthernet0/0.80
no passive-interface FastEthernet0/0.90
no passive-interface FastEthernet0/0.100
no passive-interface FastEthernet0/0.110
no passive-interface FastEthernet0/0.120
no passive-interface FastEthernet0/0.130
no passive-interface FastEthernet0/0.140
no passive-interface FastEthernet0/0.150
no passive-interface FastEthernet0/0.160
no passive-interface FastEthernet0/0.170
no passive-interface FastEthernet0/0.180
no passive-interface FastEthernet0/0.190
no passive-interface FastEthernet0/0.200
no auto-summary
```

La sentencia *network 172.16.30.0 0.0.0.127* incluye a todas las interfaces que tengan configurada una IP dentro del rango de direcciones de 172.16.30.0 a la 172.16.30.128. Se pudo haber incluido una sentencia por cada una de las redes; sin embargo, por medio de la máscara de Wildcard se logran incluir en una sentencia una red que incluya a todas las interfaces del Router (físicas o virtuales) que participarán en el proceso de EIGRP y enviar la información de todas esas redes.

Al configurar el proceso de EIGRP en el Router principal se inicia el intercambio de mensajes saludo entre los Routers de los planteles, generándose adyacencias entre Routers. Cada que se genera una nueva adyacencia con algún Router, aparece un mensaje en la terminal de configuración del Router que indica que se ha establecido una adyacencia con un Router:

%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 172.16.30.66 (FastEthernet0/0.170) is up: new adjacency

Se puede observar el resultado de las tablas de ruteo de los Routers de los planteles y del Router que los interconecta. La tabla de ruteo del Router de enlace es la siguiente después de implementarse la tabla de ruteo:

```
show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set
```

```
D       172.16.1.0/24 [90/30720] via 172.16.30.2, 00:00:38, FastEthernet0/0.10
D       172.16.2.0/24 [90/30720] via 172.16.30.6, 00:00:40, FastEthernet0/0.20
D       172.16.3.0/24 [90/30720] via 172.16.30.10, 00:00:39, FastEthernet0/0.30
D       172.16.4.0/24 [90/30720] via 172.16.30.14, 00:00:38, FastEthernet0/0.40
D       172.16.5.0/24 [90/30720] via 172.16.30.18, 00:00:39, FastEthernet0/0.50
D       172.16.6.0/24 [90/30720] via 172.16.30.22, 00:00:39, FastEthernet0/0.60
D       172.16.7.0/24 [90/30720] via 172.16.30.26, 00:00:39, FastEthernet0/0.70
D       172.16.8.0/24 [90/30720] via 172.16.30.30, 00:00:28, FastEthernet0/0.80
D       172.16.9.0/24 [90/30720] via 172.16.30.34, 00:00:38, FastEthernet0/0.90
D       172.16.10.0/24 [90/30720] via 172.16.30.38, 00:00:40, FastEthernet0/0.100
D       172.16.11.0/24 [90/30720] via 172.16.30.42, 00:00:40, FastEthernet0/0.110
D       172.16.12.0/24 [90/30720] via 172.16.30.46, 00:00:40, FastEthernet0/0.120
D       172.16.13.0/24 [90/30720] via 172.16.30.50, 00:00:40, FastEthernet0/0.130
D       172.16.14.0/24 [90/30720] via 172.16.30.54, 00:00:38, FastEthernet0/0.140
D       172.16.15.0/24 [90/30720] via 172.16.30.58, 00:00:38, FastEthernet0/0.150
D       172.16.16.0/24 [90/30720] via 172.16.30.62, 00:00:38, FastEthernet0/0.160
D       172.16.17.0/24 [90/30720] via 172.16.30.66, 00:00:37, FastEthernet0/0.170
D       172.16.18.0/24 [90/30720] via 172.16.30.70, 00:00:39, FastEthernet0/0.180
D       172.16.19.0/24 [90/30720] via 172.16.30.74, 00:00:39, FastEthernet0/0.190
D       172.16.20.0/24 [90/30720] via 172.16.30.78, 00:00:38, FastEthernet0/0.200
C       172.16.30.0/30 is directly connected, FastEthernet0/0.10
<Resultados omitidos, redes conectadas directamente, las subinterfaces>
```

Se puede observar que hay veinte entradas más en la tabla de ruteo además de las redes conectadas directamente. Estas entradas nuevas están denotadas con la letra “D” al inicio, esto indica que son fuentes generadas por Routers que tiene configurado el protocolo EIGRP, ya que este protocolo trabaja utilizando el algoritmo DUAL.

Asimismo, se podrá observar la tabla de vecinos con los que se ha establecido adyacencia el Router. Los Routers vecinos utilizan la dirección IP de la interfaz que enlaza al Router con su vecino.

```
ROUTER# show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address         Interface      Hold Uptime    SRTT   RTO   Q   Seq
(sec)          (ms)        CntNum
0   172.16.30.38                     14   00:13:03  40     1000  0   343
1   172.16.30.6                      11   00:13:03  40     1000  0   400
2   172.16.30.26                     12   00:13:02  40     1000  0   343
3   172.16.30.62                     10   00:13:02  40     1000  0   343
4   172.16.30.50                     13   00:13:02  40     1000  0   343
5   172.16.30.54                     12   00:13:02  40     1000  0   343
6   172.16.30.42                     12   00:13:01  40     1000  0   404
7   172.16.30.22                     10   00:13:01  40     1000  0   343
8   172.16.30.58                     13   00:13:01  40     1000  0   343
9   172.16.30.18                     10   00:13:01  40     1000  0   343
10  172.16.30.46                     12   00:13:01  40     1000  0   343
11  172.16.30.74                     14   00:13:00  40     1000  0   402
12  172.16.30.10                     11   00:13:00  40     1000  0   332
13  172.16.30.70                     11   00:13:00  40     1000  0   343
14  172.16.30.66                     10   00:13:00  40     1000  0   343
15  172.16.30.14                     11   00:13:00  40     1000  0   386
16  172.16.30.34                     12   00:12:59  40     1000  0   343
17  172.16.30.2                      13   00:12:59  40     1000  0   343
18  172.16.30.78                     12   00:12:59  40     1000  0   343
19  172.16.30.30                     10   00:12:50  40     1000  0   388
ROUTER#
```

El Router de enlace ha creado adyacencias con veinte Routers, correspondientes a los planteles del IEMS conectados al Router de salida. De la misma manera, los Routers de cada plantel han convergido en su tabla de ruteo

y ahora tiene una ruta hacia cada plantel y su red local correspondiente. La tabla de ruteo que ha convergido se muestra a continuación, como ejemplo la tabla de ruteo del dispositivo del plantel 3:

```
Plantel-3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external  type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.16.30.9 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 41 subnets, 2 masks
D       172.16.1.0/24 [90/33280] via 172.16.30.9, 00:22:14, FastEthernet0/0
D       172.16.2.0/24 [90/33280] via 172.16.30.9, 00:21:59, FastEthernet0/0
C       172.16.3.0/24 is directly connected, FastEthernet0/1
D       172.16.4.0/24 [90/33280] via 172.16.30.9, 00:21:53, FastEthernet0/0
D       172.16.5.0/24 [90/33280] via 172.16.30.9, 00:21:58, FastEthernet0/0
D       172.16.6.0/24 [90/33280] via 172.16.30.9, 00:21:55, FastEthernet0/0
D       172.16.7.0/24 [90/33280] via 172.16.30.9, 00:22:13, FastEthernet0/0
D       172.16.8.0/24 [90/33280] via 172.16.30.9, 00:21:57, FastEthernet0/0
D       172.16.9.0/24 [90/33280] via 172.16.30.9, 00:21:53, FastEthernet0/0
D       172.16.10.0/24 [90/33280] via 172.16.30.9, 00:21:47, FastEthernet0/0
D       172.16.11.0/24 [90/33280] via 172.16.30.9, 00:21:50, FastEthernet0/0
D       172.16.12.0/24 [90/33280] via 172.16.30.9, 00:21:48, FastEthernet0/0
D       172.16.13.0/24 [90/33280] via 172.16.30.9, 00:21:49, FastEthernet0/0
D       172.16.14.0/24 [90/33280] via 172.16.30.9, 00:22:13, FastEthernet0/0
D       172.16.15.0/24 [90/33280] via 172.16.30.9, 00:22:13, FastEthernet0/0
D       172.16.16.0/24 [90/33280] via 172.16.30.9, 00:21:56, FastEthernet0/0
D       172.16.17.0/24 [90/33280] via 172.16.30.9, 00:21:59, FastEthernet0/0
D       172.16.18.0/24 [90/33280] via 172.16.30.9, 00:21:51, FastEthernet0/0
D       172.16.19.0/24 [90/33280] via 172.16.30.9, 00:21:55, FastEthernet0/0
D       172.16.20.0/24 [90/33280] via 172.16.30.9, 00:21:49, FastEthernet0/0
D       172.16.30.0/30 [90/30720] via 172.16.30.9, 00:22:13, FastEthernet0/0
D       172.16.30.4/30 [90/30720] via 172.16.30.9, 00:22:13, FastEthernet0/0
C       172.16.30.8/30 is directly connected, FastEthernet0/0
D       172.16.30.12/30 [90/30720] via 172.16.30.9, 00:22:13, FastEthernet0/0
D       172.16.30.16/30 [90/30720] via 172.16.30.9, 00:22:13, FastEthernet0/0
D       172.16.30.20/30 [90/30720] via 172.16.30.9, 00:22:13, FastEthernet0/0
D       172.16.30.24/30 [90/30720] via 172.16.30.9, 00:22:13, FastEthernet0/0
D       172.16.30.28/30 [90/30720] via 172.16.30.9, 00:22:13, FastEthernet0/0
D       172.16.30.32/30 [90/30720] via 172.16.30.9, 00:22:13, FastEthernet0/0
D       172.16.30.36/30 [90/30720] via 172.16.30.9, 00:22:13, FastEthernet0/0
D       172.16.30.40/30 [90/30720] via 172.16.30.9, 00:22:13, FastEthernet0/0
D       172.16.30.44/30 [90/30720] via 172.16.30.9, 00:22:13, FastEthernet0/0
D       172.16.30.48/30 [90/30720] via 172.16.30.9, 00:22:13, FastEthernet0/0
D       172.16.30.52/30 [90/30720] via 172.16.30.9, 00:22:13, FastEthernet0/0
D       172.16.30.56/30 [90/30720] via 172.16.30.9, 00:22:13, FastEthernet0/0
D       172.16.30.60/30 [90/30720] via 172.16.30.9, 00:22:13, FastEthernet0/0
D       172.16.30.64/30 [90/30720] via 172.16.30.9, 00:22:13, FastEthernet0/0
D       172.16.30.68/30 [90/30720] via 172.16.30.9, 00:22:13, FastEthernet0/0
D       172.16.30.72/30 [90/30720] via 172.16.30.9, 00:22:13, FastEthernet0/0
D       172.16.30.76/30 [90/30720] via 172.16.30.9, 00:22:13, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 172.16.30.9
```

Cada uno de los Routers ha aprendido las rutas a las redes de los planteles, así como la de cada uno de los enlaces realizados al Router principal. De esta manera, la ruta predeterminada podría eliminarse de la configuración

que hacía al Router-on-a-stick direccionar el tráfico entre los enlaces en las VLAN. Sin embargo, se mantendrá la entrada para realizar el ruteo hacia Internet.

La tabla de vecinos para cada Router de plantel sólo contiene una entrada, este es el Router de enlace a internet, y se identifica con la dirección IP configurada en la subinterfaz correspondiente. La siguiente salida es la que corresponde a la tabla de vecinos del Router del plantel 10:

```
Plantel-10>show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address         Interface      Hold Uptime    SRTT   RTO   Q   Seq
                                   (sec)          (ms)        CntNum
0   172.16.30.37     Fa0/0          14   01:32:15  40     1000  0   457
```

Ahora todos los Routers son convergentes y tienen alcance con los demás dispositivos en la red. Se puede comprobar la comunicación ejecutando un comando PING desde la red LAN de un plantel a otro. A continuación se verifica la conectividad entre el plantel 5 dónde hay una computadora con la dirección IP 172.16.5.1 con un equipo en la red local del plantel 19, con la dirección IP 172.16.19.1:

```
PC>ipconfig

IP Address.....................: 172.16.5.10
Subnet Mask....................: 255.255.255.0
Default Gateway................: 172.16.5.254

PC>ping 172.16.19.1

Pinging 172.16.19.1 with 32 bytes of data:

Reply from 172.16.19.1: bytes=32 time=96ms TTL=125
Reply from 172.16.19.1: bytes=32 time=114ms TTL=125
Reply from 172.16.19.1: bytes=32 time=78ms TTL=125
Reply from 172.16.19.1: bytes=32 time=50ms TTL=125

Ping statistics for 172.16.19.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 50ms, Maximum = 114ms, Average = 84ms
```

En este punto todos los planteles tienen comunicación entre sí.

2.8 Escalabilidad en la red de datos

Una red institucional debe ser capaz de soportar el crecimiento de sí misma, y por lo tal, tener la habilidad de adaptarse a dicha evolución sin ningún problema. A continuación se contemplan escenarios que pudiesen presentarse durante el crecimiento de la red.

2.8.1 Crecimiento de la red

El crecimiento de la red se puede dar por las siguientes causas. Una de las más comunes es que el número de usuarios por plantel aumente, esto debido a que el número de ellos aumento por crecimiento de las instalaciones y por tal del número de dispositivos que necesitarán comunicarse entre sí y hacia el exterior.

Otro punto importante que se debe mantener en consideración es el crecimiento de la red debido a que esta aumentó en número de nodos, es decir, más planteles.

Para cada uno de esos casos, es importante conocer cuáles son los movimientos a seguir, principalmente en la distribución física, la integración lógica y protocolos.

2.8.1.1 Aumento de número de usuarios por plantel

La red del IEMS en cada uno de sus planteles tiene alrededor de no más de 200, y, actualmente para cada una de las redes en los planteles del IEMS se han planeado para brindar 254 estaciones de trabajo. Sin embargo, 8 de esas estaciones son destinadas a los administradores de red y las demás se comparten entre aulas, centro de cómputo y personal administrativo. Sin embargo, la probabilidad de crecimiento de número de usuarios en los planteles genera el requerimiento de ampliación de la red. Las 254 direcciones de red serán insuficientes, por lo que será necesaria la petición de direccionamiento a las oficinas centrales de la red.

Luego, con una red mucho más extensa en cada plantel que crece, es más probable la división de tráfico en la misma, en consecuencia, el nombre de VLAN se hace presente de nueva cuenta. Las próximas explicaciones mostrarán las configuraciones necesarias para que se lleve a cabo el crecimiento de una red local que cuenta con un Router y switches Cisco®.

La planeación de crecimiento en la red de IEMS se explicará de mejor manera suponiendo el crecimiento de uno de los planteles, en concreto, el plantel 2.

Escenario: El plantel 2 por crecimiento de instalaciones, tiene la capacidad de albergar a más alumnos y personal administrativo, por lo cual, el número de usuarios crece de 180 a 325. El actual direccionamiento que se tiene en este plantel es una red /24, es decir, con 254 direcciones de red útiles para uso en el plantel.

Antes del crecimiento, la red tenía 74 direcciones de red disponibles, pero, debido al incremento de usuarios, la red requiere 71 direcciones de red más, y un 10% adicional por crecimientos que se de en menor escala, 103 direcciones de red en total son requeridas. Si se trata del primer plantel que tiene un crecimiento, el direccionamiento que otorgarán las oficinas centrales de la red será tomado de aquel que se tiene reservado de la red 172.16.0.0, de la cual se utilizaron de la red 172.16.1.0/24 hasta la 172.16.20.0/24 para las redes locales de los 20 planteles, y de la red 172.16.30.0/30 hasta la 172.16.30.76/30 para los enlaces L2L. Existe direccionamiento que va de la dirección 172.16.21.0 hasta la dirección 172.16.29.255 de direcciones que quedaron reservadas para crecimiento de las redes locales, un total de 2550 direcciones de red, contando ID de red y dirección de broadcast.

Este requerimiento podrá ser cubierto tomando el segmento de red 172.16.21.0/25 de las redes contenidas entre las direcciones que quedarán disponibles entre las redes de los planteles y los enlaces L2L. Esta red /25 ofrecerá la cantidad de 126 direcciones de red útiles, con 23 direcciones de red más de lo que se requiere.

Tabla 2.8. Direccionamiento asignado en el proceso de crecimiento de plantel.

Departamento	Segmentos de red	Total de direcciones	VLAN
Red Educativa	172.16.2.0/24 (menos las direcciones de los administradores de red) 172.16.21.0/26 172.16.21.64/27	339 útiles	10,20,30
Dirección plantel	172.16.21.96/27	30 útiles	100
Administradores de red	172.16.2.248 a la 172.16.2.254	7 útiles	10

De esta manera, el plantel 2 cuenta con dos segmentos de red, el 172.16.2.0/24 y el 172.16.21.0/25, haciendo un total de 384 direcciones, menos identificadores de red y direcciones de broadcast. De estos segmentos, se utilizará todo el segmento 172.16.2.0 para la asignación en equipos de aulas y centro de cómputo, y se mantendrán las direcciones de IP de los administradores de red (un cambio equivale a cambiar las listas de acceso en todos los Routers de la red). Los primeros tres cuartos del segmento 172.16.21.0/25 serán utilizado para aulas y centros de cómputo, y el resto de las direcciones IP serán destinados a empleados de la dirección y personal secretarial.

Es posible notar en la tabla anterior la asignación de una VLAN a cada uno de los departamentos o áreas de la red del plantel, esto se hace necesario para la segmentación del tráfico ya que serán diferentes por el tipo de usuarios en cada una de ellas y se vuelve importante debido a que el crecimiento de la red se ha presentado.

La topología de la red en el plantel 2 antes del crecimiento se puede observar en la figura 2.16.

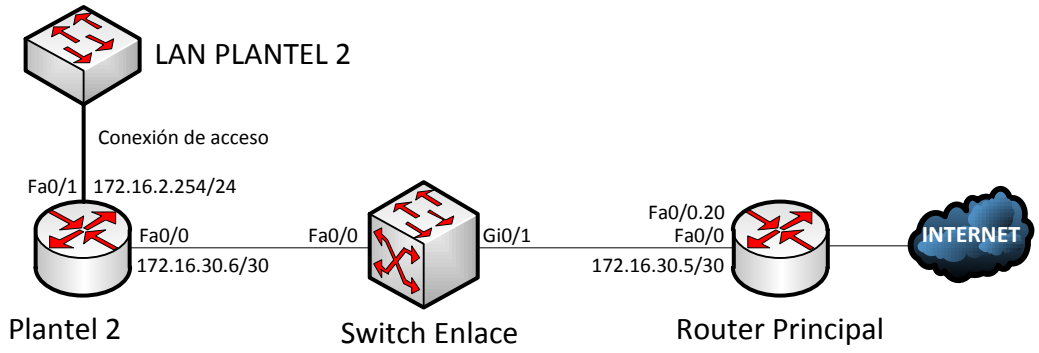

Figura 2.44 Topología de Álvaro Obregón antes del crecimiento

La configuración del Router del Plantel 2 es la siguiente en el esquema anterior: Se tiene una de las interfaces en el enlace L2L, y otra a la red local, esta última configurada con un rango de direccionamiento para asignación dinámica de direcciones IP a través de DHCP.

```
ip dhcp excluded-address 10.30.2.248 10.30.2.254
ip dhcp pool LANPLANTEL2
 network 172.16.2.0 255.255.255.0
 default-router 172.16.2.254
```

La interfaz que está conectada a la red local tiene sólo una descripción, y la última dirección de red del segmento que se asignó.

```
interface FastEthernet0/1
 description LAN_PLANTEL_2
 ip address 172.16.2.254 255.255.255.0
```

La configuración del proceso de EIGRP está definido con el mismo número de sistema autónomo (en una red pequeña en la que se implementa un protocolo de gateway interior, IGP, no precisamente es un sistema autónomo, es sólo el ID con el que se definirá el proceso de ruteo en el dispositivo), el cual será 100 en toda la red. Sólo se estarán anunciando la red local y la red del enlace L2L.

```
router eigrp 100
 passive-interface default
 no passive-interface FastEthernet0/0 ! Interfaz conectada al enlace L2L
 network 172.16.2.0 0.0.0.255          ! Anuncio de la red local
 network 172.16.30.4 0.0.0.3           ! Anuncio de la red del enlace L2L
 no auto-summary
!
```

Al lanzarse el requerimiento de crecimiento de la red, se tiene que establecer un plan de cambio de la misma, en el que el direccionamiento se encuentra involucrado. La conexión física que se tiene entre el Switch y el Router del plantel se mantiene igual, pero la configuración de la interfaz del Router cambia, dividiéndose en subinterfaces, una perteneciente a cada segmento de la red.

La configuración del Switch cambia también. Originalmente se tenía un dispositivo sin configuración, la configuración predeterminada de fábrica era suficiente, sin embargo, como se ha implementado el concepto de VLAN, es necesaria que la interfaz que conecta con el Router cambie a modo troncal, para que todas las subredes tengan la posibilidad de salir a través del Router.

Se dividirá la interfaz del Router en subinterfaces según el número de subredes que se desee. Por ejemplo, si se desea que la red 172.16.2.0/24 sea dividida en subredes, una por cada aula en el plantel, será necesaria la creación de tantas subinterfaces como subredes que se haya dividido el segmento.

El arreglo de switches que conecte a cada estación de trabajo, debe de tener configurada la VLAN correspondiente a la que da acceso, así como asignados los puertos correspondientes a la VLAN indicada. Figura 2.17.

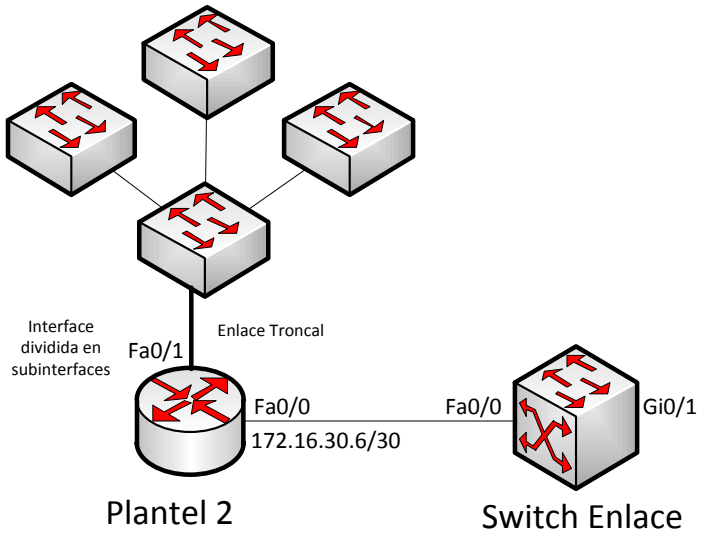

Figura 2.45 Crecimiento de la red local

La configuración de los dispositivos es muy sencilla; sin embargo, el paso complicado del crecimiento de la LAN en un plantel es la construcción del cableado estructurado y la conexión de los dispositivos. Esta conexión física depende de la distribución de los páneles de parcheo a los nodos de red que conectará a cada una de las estaciones de trabajo. Si el cuarto de telecomunicaciones se encuentra bien construido y distribuido de la manera más adecuada entre los páneles de parcheo y el cableado, la activación de cualquier nodo es muy sencilla, sólo se requiere que se solicite al administrador de la red que encienda el puerto y lo asigne a la VLAN que corresponda según el rol del usuario que solicite.

El cambio de configuración se da a la siguiente:

```
ip dhcp excluded-address 10.30.2.248 10.30.2.254

ip dhcp pool LANPLANTEL2
 network 172.16.2.0 255.255.255.0
 default-router 172.16.2.254

ip dhcp pool LANPLANTEL2_1
 network 172.16.21.0 255.255.255.192
 default-router 172.16.21.62

ip dhcp pool LANPLANTEL2_3
 network 172.16.21.64 255.255.255.224
 default-router 172.16.21.94

ip dhcp pool ADMINISTRATIVOS
 network 172.16.21.96 255.255.255.224
 default-router 10.30.21.126
interface FastEthernet0/1
 description LAN PLANTEL 2
 no ip address
 no shutdown
!
```

```
interface FastEthernet0/1.10
 description LAN PLANTEL 2
 encapsulation dot1Q 10
 ip address 172.16.2.254 255.255.255.0
!

interface FastEthernet0/1.20
 description LAN PLANTEL 2
 encapsulation dot1Q 20
 ip address 172.16.21.62 255.255.255.192
!

interface FastEthernet0/1.30
 description LAN PLANTEL 2
 encapsulation dot1Q 30
 ip address 172.16.21.94 255.255.255.224
!

interface FastEthernet0/1.100
 description ADMINISTRACION
 encapsulation dot1Q 100
 ip address 172.16.21.126 255.255.255.224
!

router eigrp 100
 passive-interface default
 no passive-interface FastEthernet0/0
 network 172.16.2.0 0.0.0.255
 network 172.16.21.0 0.0.0.127
 no auto-summary
!
```

Se crean tres conjuntos de direcciones para el servidor de DHCP para la red del plantel, llamadas LANPLANTEL2, LANPLANTEL2_1 y LANPLANTEL2_2 que asignarán a los dispositivos las direcciones de red dinámicamente. Se mantienen las direcciones IP para los equipos de los administradores; sin embargo, estás se mantendrán dentro de la misma VLAN de datos que los usuarios que tengan una dirección de red del conjunto LANPLANTEL2.

Así pues, existe un conjunto de direcciones para el servidor de DHCP para los equipos del departamento administrativo.

La configuración de la interfaz que conecta con el Switch es diferente, la interfaz física ya no contiene la dirección IP, sólo estará activada, no obstante, esta será dividida en subinterfaces, ¿cuántas?, el número de subredes que se requieran. Particularmente, este caso se utilizan cuatro subredes, cuatro subinterfaces y por tal, cuatro VLAN.

El proceso de ruteo de EIGRP no cambia nada. No obstante, para que el dispositivo no envíe tres rutas más debido a que la red 172.16.21.0/25 que se segmentó, se agrega la siguiente línea de configuración sobre la interfaz no pasiva:

```
 interface FastEthernet0/0
 ip address 10.30.30.6 255.255.255.252
 ip summary-address eigrp 100 172.16.21.0 255.255.255.128 5
```

Donde se indica a la interfaz que a través del proceso de eigrp 100 se enviará la red 10.30.21.0/25 con una distancia administrativa de cinco. Así que, la ruta aparecerá en la tabla de ruteo de la siguiente forma en los demás equipos, en concreto, el Router del plantel 4:

```
D       172.16.21.0/25 [90/33280] via 172.16.30.13, 00:03:10, FastEthernet0/0
```

La entrada es una sola ruta. Si no se hubiese sumarizado a través de dicha sentencia, las entradas en las tablas de ruteo para las nuevas redes como se muestra a continuación:

```
D       172.16.21.0/26 [90/33280] via 172.16.30.13, 00:00:09, FastEthernet0/0
D       172.16.21.64/27 [90/33280] via 172.16.30.13, 00:00:09, FastEthernet0/0
D       172.16.21.96/27 [90/33280] via 172.16.30.13, 00:00:09, FastEthernet0/0
```

La distancia administrativa que se define en la sintaxis del comando para esta red no tiene relevancia, ya que sólo hay un protocolo de ruteo que la anuncia, este valor sería importante si en el dispositivo hubieran más protocolos de ruteo configurados anunciando las mismas redes además de EIGRP.

Con respecto a la configuración del Switch en comparación al arreglo de switches que se pudo haber utilizado con la red pequeña sin la necesidad de establecer una configuración específica en el dispositivo, la ampliación de la red local genera la necesidad de la creación de VLANs y la configuración de enlaces troncales entre los switches y entre switches y Routers. Para muestra la configuración de las VLAN en el Switch del plantel 2 después del crecimiento de la red:

```
Switch(config-vlan)#name RED1
Switch(config-vlan)#VLAN 20
Switch(config-vlan)#name RED2
Switch(config-vlan)#VLAN 30
Switch(config-vlan)#name RED3
Switch(config-vlan)#VLAN 100
Switch(config-vlan)#name ADMINISTRATIVOS
```

Ahora bien, después de configuradas las VLAN en el dispositivo, se hace necesaria la asignación de puertos a las VLAN correspondientes. De esta manera, el puerto asignado a la VLAN correspondiente tendrá la capacidad de comunicarse con dispositivos en la misma VLAN, con determinados parámetros de red asignados según la VLAN en la que se encuentre el usuario.

```
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode trunk
!
```

Esta configuración de los puertos que conectan al Switch con el Router permite el paso del tráfico de las VLAN a través de un mismo canal. La conexión entre switches será por medio de un enlace troncal, no así los puertos a los que se conecten las estaciones de trabajo, la configuración de estos será como modo de “acceso” e indicar la VLAN a la que estará asociada la red.

La configuración de un puerto será como se muestra a continuación:

```
interface FastEthernet0/21
 switchport access vlan 20
 switchport mode access
!
```

Las líneas encima muestran la configuración de un puerto que conectará a un equipo sobre la VLAN 20, es decir, esta red tendrá una dirección IP de la red 172.16.21.0/26. Este equipo tendrá correspondencia con la subinterfaz en el Router que encapsula en la VLAN 20, se identificará la dirección IP de la subinterfaz, y gracias a esta se le asignará una dirección IP del pool correspondiente. En este caso, el equipo recibirá una dirección de red del pool de DHCP LANPLANTEL2_1.

2.8.1.2 Incremento en el número de planteles

Esta red puede sufrir crecimiento de usuarios en cada plantel, misma que ya se trató en el punto anterior; sin embargo, la red también puede crecer si se añade uno o más planteles más.

Actualmente se cuentan con 20 planteles, todos se conectan a través de enlaces Lan-to-Lan (L2L) a un Switch de alta velocidad que a la vez se conecta a un Router que les da salida a la red de Internet. En este esquema, tanto el Switch de alta velocidad, así como los enlaces L2L son proporcionados por un proveedor de servicios. Además, este Switch del proveedor tiene la capacidad de recibir 20 enlaces solamente, razón por la cual, en caso de presentarse la adición de un nuevo plantel, se solicitará al proveedor la instalación de un nuevo Switch con mayor capacidad para sustituir el ya instalado. Veámoslo mediante un ejemplo, en el caso de que se genere un nuevo plantel, el Switch ya no tiene la capacidad para albergar, se solicitaría el cambio por un nuevo Switch con 6 puertos más, entonces, se tendrán 5 puertos más para la adición de más planteles.

Un inconveniente de la sustitución del Switch de alta velocidad es que, durante el cambio de Switch, habrá afectación de servicio debido a que todos los enlaces se tendrán que retirar y activar de nuevamente en el nuevo dispositivo y los enlaces, considerando el nuevo.

Después de haber realizado la conexión del nuevo dispositivo con el Router, la interfaz de este último se dividirá en una nueva subinterfaz, asignándole una nueva VLAN y el direccionamiento correspondiente proveniente de un segmento consecutivo de los últimos utilizados por los enlaces L2L.

Otra de las opciones es la adquisición de un nuevo Switch de alta velocidad, con un menor número de puertos, y conectar al Router de la misma forma que el anterior. A través de este nuevo dispositivo, los planteles que se vayan agregando se podrán conectar en él.

Las consideraciones de lo anterior descrito, el Router debe de contar con las interfaces suficientes para este movimiento. Así bien, también es importante tener las interfaces adecuadas (en capacidad y velocidades) para que se garantice el efectivo transporte del volumen de tráfico generado por las redes locales y protocolos que conviven en la red.

La topología de esta última solución descrita queda planteada en la figura 2.18.

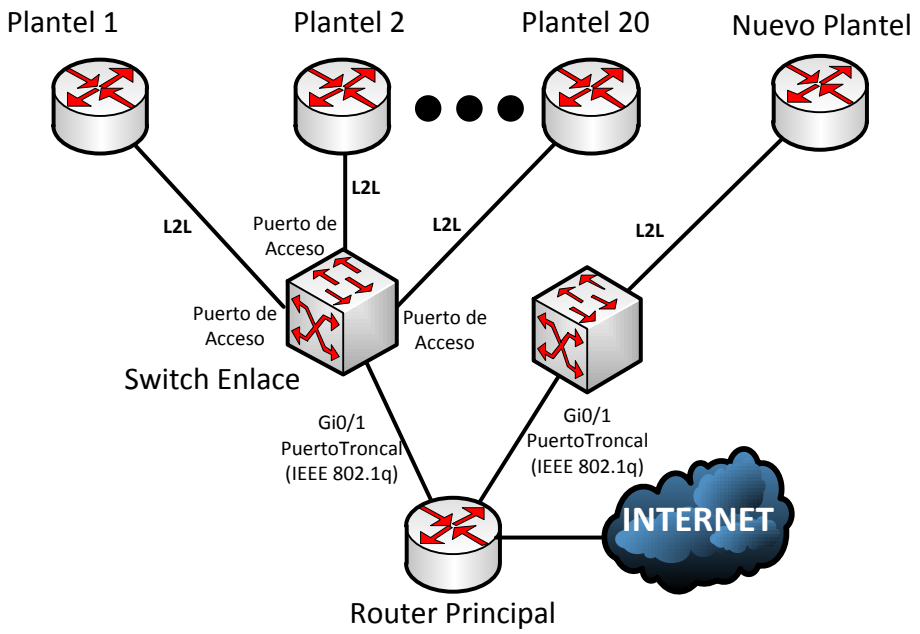

Figura 2.46 Adición de un nuevo Switch a la red

La configuración de la interfaz al nuevo Switch es totalmente la misma que el primer Switch que estará operando. Mientras se adicionen nuevos planteles, la interfaz del Router que interconecta con el Switch se dividirá en subinterfaces. Con todo ese cambio, también la configuración de ruteo es la misma, las redes a anunciar se indican en el mismo proceso de EIGRP.

Se considera que el nuevo plantel ha sido conectado por medio de un Router también de marca Cisco®, pero, ¿qué sucede cuándo el Router es de otro fabricante?

2.8.2 Redistribución

Debido a que la red presentará crecimiento, la introducción de nuevos dispositivos a la misma es inevitable; Sin embargo, como se mencionó en el punto 2.8.1 de este documento, el protocolo de ruteo a utilizarse es EIGRP, un protocolo propietario de Cisco®, por lo que, esto determina que los dispositivos a utilizarse son provistos por esa empresa.

Se ha tomado la decisión de utilizar EIGRP sobre OSPF debido a que se planea que durante el crecimiento involucre que dispositivos de la marca Cisco® ingresen a la red. EIGRP cuenta con mayor número de factores para elegir la mejor ruta a su destino que RIP. RIP usa el número de saltos como métrica, mientras que EIGRP utiliza el ancho de banda, el retardo, la carga y la confiabilidad del enlace y en una red institucional como la del IEMS, el protocolo es el idóneo para su implementación.

Se debe tener en cuenta que en el caso de que se tenga la red completamente implementada sobre una infraestructura Cisco®, existe la posibilidad de que durante la ampliación de la red a nuevos planteles o la falla del Router de salida de alguno de los planteles en operación, se cuente con un Router de respaldo de una marca distinta, y, por obvias razones no soportará el protocolo de ruteo de EIGRP utilizado en la red completa. En este caso, Cisco® a través de EIGRP ofrece una característica de ruteo llamado “Redistribución”.

Hoy en día muchas redes de datos usan un solo protocolo de ruteo y aprenden rutas a través del él; sin embargo, en algunos casos, las rutas aprendidas por un IGP deben de ser anunciadas a otro IGP distinto, y viceversa. Una

solución empleada para este requerimiento es la de tomar las rutas aprendidas por un protocolo de ruteo y anunciarlas dentro de otro protocolo de ruteo, y esta es una solución que provee el sistema operativo IOS de Cisco®. De esta manera, la red que utiliza EIGRP anunciará las rutas al Router que maneja RIP por medio de distribución.

La red que se ha planeado en este documento está planeada en su implementación completa por Routers de marca Cisco®, y, cuando se ejecute la acción de mejora, el protocolo de enrutamiento a utilizar es EIGRP, un protocolo propietario de Cisco®. Sin embargo, debido al crecimiento de la red de datos, es posible que algún dispositivo nuevo que ingrese a la no sea del proveedor Cisco®, este no podrá compartir información de ruteo con los demás debido a que EIGRP sólo puede ser configurado en dispositivos de la marca Cisco®; pero, en esa situación, se propone el uso de RIP en su versión en el dispositivo nuevo porque es un protocolo que tiene la capacidad necesaria para que la red siga cumpliendo con la convergencia rápida.

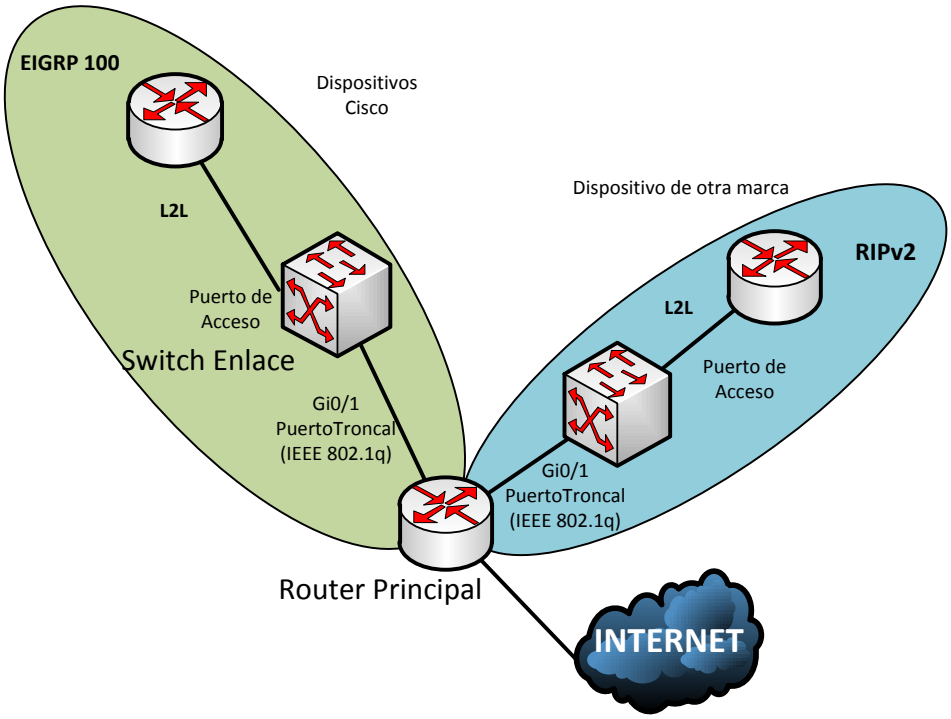

Figura 2.47 Conexión de una red sobre RIPv2 a otra sobre EIGRP

En el caso de adicionarse un nuevo plantel con un Router de marca Cisco®, no habrá ningún problema en configurar EIGRP para integrar el plantel al dominio de ruteo, no obstante, en el caso de presentarse la conexión con un Router de una marca distinta, el protocolo utilizado será RIP, mientras que en el Router de enlaces se le configurará el protocolo RIP con redistribución de redes de EIGRP, y EIGRP con redistribución de rutas de RIP, de esa manera, ambos dominios de ruteo se conectan. Figura 2.19.

Lo descrito anteriormente se ejemplificará con el escenario siguiente:

Escenario: Un nuevo plantel da apertura, se adiciona un Switch nuevo por lo cual se realiza el enlace L2L entre el plantel nuevo y el Router principal en las oficinas centrales. Sin embargo, debido a la escasez de presupuesto, se cuenta en la bodega con un Router que ofrece la capacidad, pero es una marca distinta a la que se utiliza en la red.

Se toma la red 172.16.30.128/30 para la configuración del enlace L2L, y la LAN del plantel con la red 172.16.25.0/24.

El Router del plantel nuevo se configura de la siguiente manera, interfaz y protocolo de ruteo:

```
ip dhcp excluded-address  172.16.21.248  172.16.21.254
!
ip dhcp pool LANPLANTEL21
 network  172.16.25.0 255.255.255.0
 default-router  172.16.25.254

interface FastEthernet0/0
 ip address  172.16.30.130 255.255.255.252
!
interface FastEthernet0/1
 description LAN PLANTEL 21
 ip address  172.16.25.254 255.255.255.0
!
router rip
 version 2
 network  172.16.0.0
!
```

La configuración es sencilla, la configuración del Router principal es la siguiente:

```
interface FastEthernet0/1.125
 encapsulation dot1Q 210
 ip address 172.16.30.129 255.255.255.252
!

router eigrp 100
 redistribute rip metric 100000 1 255 1 1500
!
router rip
 version 2
 redistribute eigrp 100 metric transparent
 passive-interface default
 no passive-interface FastEthernet0/1.125
 network 172.16.0.0
!
```

En el proceso de EIGRP 100, la línea *redistribute rip metric 100000 1 255 1 1500* indica al proceso de EIGRP que se redistribuirá información del protocolo de ruteo RIP con una métrica con el siguiente conjunto de parámetros configurados: 100000 kBits de ancho de banda, un retardo de una unidad de 10 microsegundos, una confiabilidad de 100% (255 es la más alta, 0 es sin confiabilidad), Ancho de banda efectivo de 1% y un valor de MTU de 1500. Estos valores construyen la entrada de las rutas de OSPF en las tablas formadas por EIGRP. En esta topología, sólo hay una ruta a la red, por lo que es irrelevante el cálculo de los parámetros.

El protocolo RIP está definido de manera normal para que se establezca el enlace con el nuevo plantel, en cambio, una línea diferente es la "*redistribute eigrp 100 metric transparent*" que le indica al protocolo que envíe las rutas de las subredes que se están anunciadas por el proceso de EIGRP 100.

De esta manera, en el Router del plantel nuevo se encontrarán entradas como esta en la tabla de ruteo, una entrada por cada red local y enlace que existe en la red:

```
<Se omiten resultados de la salida del comando>
.
R       172.16.0.0/16 [120/1] via 172.16.30.129, 00:00:09, FastEthernet0/0
R       172.16.30.0/30 [120/1] via 172.16.30.129, 00:00:09, FastEthernet0/0
R       172.16.30.4/30 [120/1] via 172.16.30.129, 00:00:09, FastEthernet0/0
R       172.16.30.8/30 [120/1] via 172.16.30.129, 00:00:09, FastEthernet0/0
R       172.16.30.12/30 [120/1] via 172.16.30.129, 00:00:09, FastEthernet0/0
.
<Se omiten resultados de la salida del comando>
```

Las rutas del nuevo plantel se ven por RIP con ningún despliegue adicional que indique que son proveniente de una distribución.

Para OSPF, las entradas en la tabla de ruteo vendrán precedidas de un O E2, la letra O se refiere que son fuente del protocolo de ruteo OSPF, y la letra E que proviene de un protocolo de ruteo externo, puede ser BGP, RIP, o como se está realizando en este caso, EIGRP, de estas rutas existen dos tipos, E1 y E2, el tipo que se utiliza en este caso son tipo 2 (E2), tienen una métrica predeterminada de 20 (llamado costo distribuido), mientras que las rutas tipo 1 son el costo distribuido más el costo a llegar al ASBR.

Mientras que en los planteles con los Routers que ejecutan el protocolo de ruteo EIGRP tienen dos entradas adicionales:

```
<Se omiten resultados de la salida del comando>
.
D EX    172.16.21.0/24 [170/28416] via 172.16.30.13, 00:01:26, FastEthernet0/0
D EX    172.16.30.128/30 [170/28416] via 172.16.30.13, 00:01:42, FastEthernet0/0
.
<Se omiten resultados de la salida del comando>
```

Estas entradas se identifican por aparecer con un "EX" en la tabla de ruteo.

De esta manera, todos los Routers comparten información de ruteo, el Router principal tiene la capacidad de anunciar rutas de EIGRP a Routers que trabajan OSPF y viceversa, sin alguna configuración adicional del lado del Router del plantel.

2.8.3 Esquema de redundancia de la salida a Internet

Uno de los problemas más graves que se presentan con esta topología es la disponibilidad de los enlaces de salida a Internet. En caso de que ocurra una falla en el equipo que proporciona esta salida, la red completa se queda sin acceso a redes externas.

Por tal razón se propone un esquema de redundancia a nivel físico. Es decir, colocar dos puntos geográficos de salida, si se pierde el sitio central por alguna catástrofe o algún incidente, los planteles se mantendrán saliendo a Internet a través del respaldo.

Este esquema es caro económicamente debido a que se tiene que colocar un enlace L2L a cada uno de los planteles. Asimismo, para aprovechar la infraestructura que ofrecerá la conectividad es necesario eliminar de todos los Routers de los planteles las rutas estáticas predeterminadas ya que por medio del protocolo de enrutamiento los dispositivos conectados a los enlaces de internet propagarán una ruta predeterminada por medio del protocolo de enrutamiento.

El esquema propuesto se muestra en la figura siguiente:

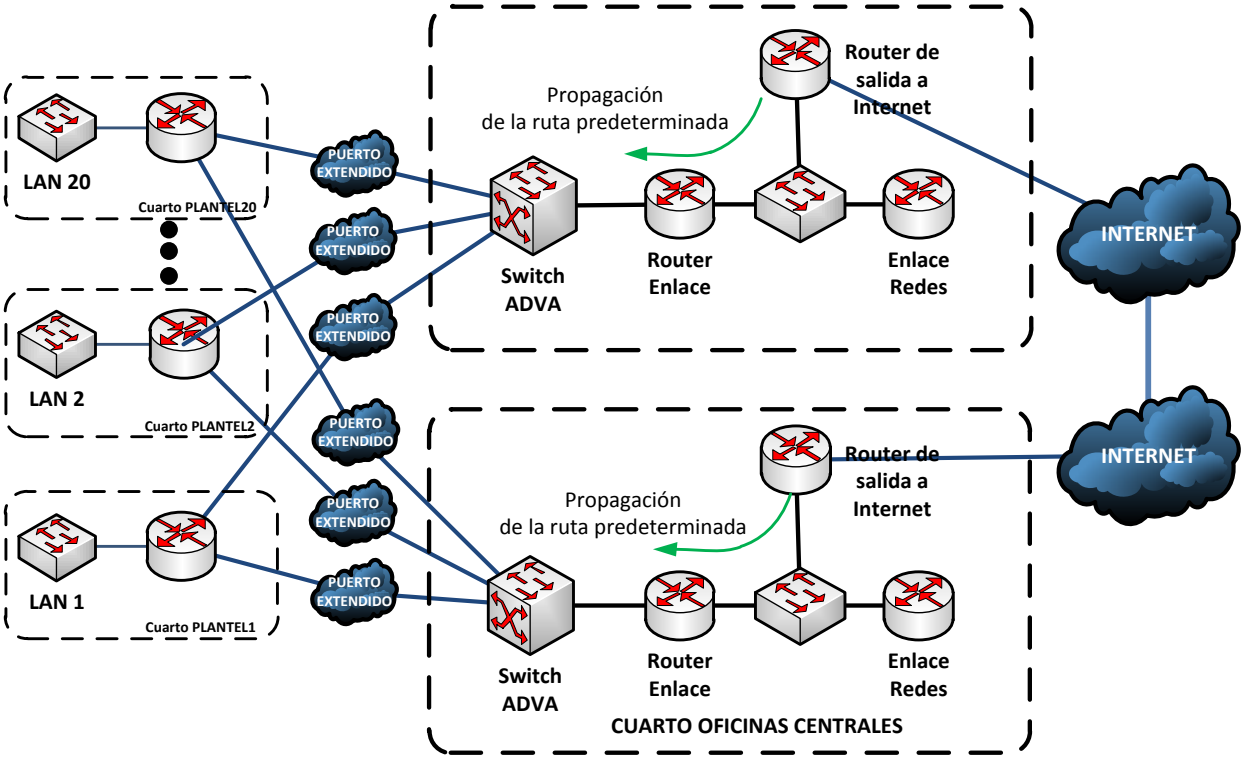

Figura 2.48 Redundancia física.

Para que el esquema red anterior funcione, es necesaria la desconfiguración de las rutas estáticas por defecto en todos los planteles, excepto el equipo de Salida a Internet, que tendrá habilitado EIGRP para el intercambio de la ruta predeterminada.

```
router eigrp 100
 redistribute static metric 100000 1 255 1 1500
```

Esta ruta se propagará hacia todos los equipos de la red. EIGRP la considera una ruta externa, por lo que su distancia administrativa es de 170. De esta forma, cada plantel de la red contará con dos salidas hacia Internet, y en caso de la pérdida de una de ellas, la ruta estática predeterminada sigue aprendiéndose por la que queda activa. De esta manera se logra que exista redundancia en la red. A continuación se muestra la ruta predeterminada y las dos salidas predeterminadas a Internet.

```
D*EX 0.0.0.0/0 [170/30976] via 172.16.120.5, 01:22:45, FastEthernet1/0
                           [170/30976] via 172.16.30.5, 01:22:43, FastEthernet0/0
```

Como se puede observar, cada equipo que cuente con dos enlaces L2L, uno a cada una de las salidas a Internet, tendrá dos rutas predeterminadas que garantizan que haya balanceo de tráfico. Por esta razón, los enlaces hacia Internet deben de tener la misma capacidad para que no haya problemas de asimetría en la red.

Por otra parte, los planteles que permanezcan con un solo enlace L2L como su salida a Internet, para no perder por completo la salida a Internet, se tendrá una conexión a un módem de DSL de cualquier proveedor de servicios como un respaldo momentáneo mientras se restablece el enlace que daba salida a la red LAN de ese nodo. Esto queda representado en la **figura**.

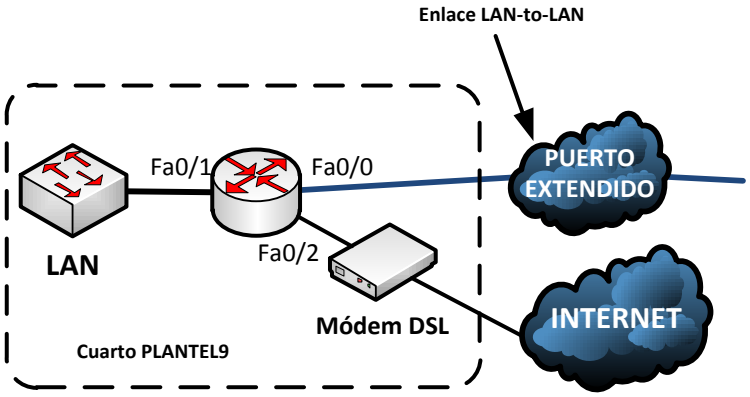

Figura 2.49. **Conexión del Router de plantel al enlace L2L y Módem DSL.**

Para que el esquema de red planteado en los planteles funcione, se tiene que realizar cierta configuración que permita la salida hacía Internet cuando el enlace L2L se pierda. Esto es posible con una ruta estática. A continuación se presenta la configuración de la Interfaz que se conectará al módem de DSL.

```
interface FastEthernet0/2
 ip address dhcp
```

La dirección IP se obtendrá de manea dinámica provista por el módem. Esta dirección será de direccionamiento privado.

La configuración de la ruta estática será a la ruta predeterminada. Una ruta estática tiene una distancia administrativa de 1. Asimismo, el Router aprende una ruta predeterminada a través del enlace L2L por medio del protocolo de EIGRP con una distancia administrativa de 170. Por tal razón, la ruta estática al módem se configurará con una distancia administrativa de 200, mayor a la del protocolo de EIGRP externo para que sea respaldo de la anterior.

```
ip route 0.0.0.0 0.0.0.0 FastEthernet0/2 200
```

Y no sólo esa configuración será suficiente. Además de permitir la salida a Internet por medio del Módem de DSL a la red en caso de fallo del enlace L2L, se determinará que el tráfico saliente sea web por medio de una lista de control de acceso que debe de ser aplicada a la interfaz para el tráfico de salida.

```
ip access-list extended TRAFICO_A_MODEM
 permit tcp 172.16.0.0 0.0.255.255 any eq www
 permit tcp 10.0.0.0 0.255.255.255 any eq 443
 permit icmp any any echo
 deny ip any any
```

```
interface FastEthernet0/2
 ip access-group TRAFICO_A_MODEM out
!
```

2.8.4 Esquema de redundancia en la red local

La red local de cada plantel y de la red de las oficinas centrales dará conexión a los host o computadoras personales a través de la red alámbrica creada con switches. Sin embargo, también es importante garantizar que esta red de switches tenga redundancia en caso de que alguno de los switches deje de funcionar o alguno de los cables que interconectan a los dispositivos se dañe.

No obstante, una red de switches con enlaces redundantes puede generar loops que provoquen que la red sea inestable en sus tablas de direcciones MAC, tenga pérdidas de tramas o duplicación de las mismas, y por tal, un incremento en el uso de CPU de los dispositivos y un uso excesivo de ancho de banda de los enlaces.

El diseño de conexión propuesto en la red será redundante; antes bien, se diseñará esta red y se establecerán las configuraciones necesarias para que el protocolo de spanning-tree rápido trabaje en esta red.

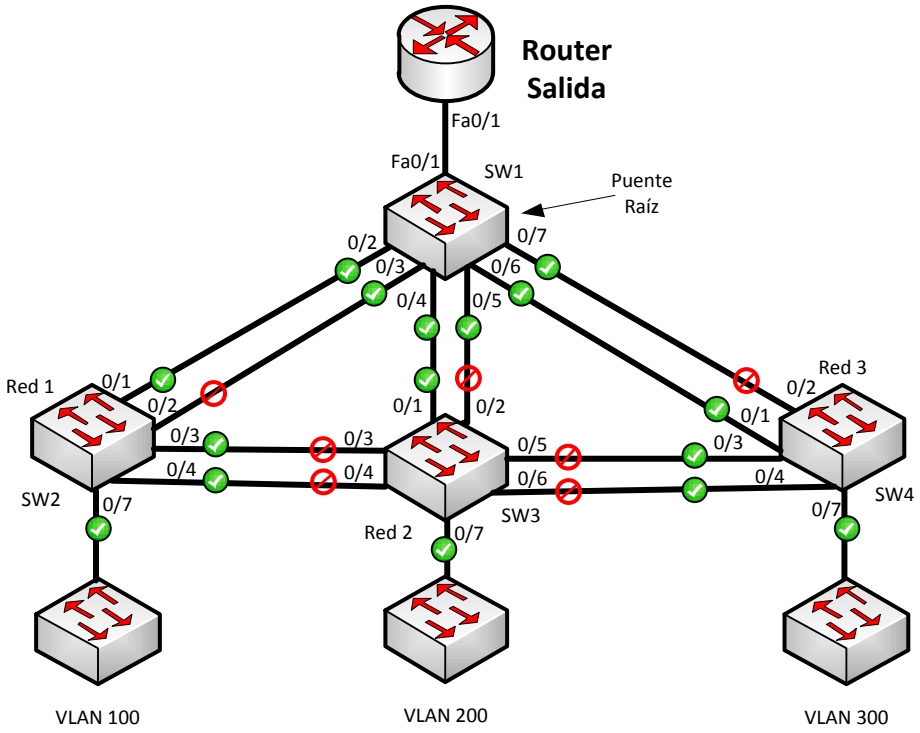

Figura 2.50. Red LAN con tres VLAN en funcionamiento.

En la 2.21 se muestra las conexiones de la LAN. Todos los enlaces entre los switches son troncales. Sin embargo, en este esquema de red es importante la selección del puente raíz que tiene que ser el más cercano al Router que reenvía la información hacia el exterior. En caso de que no se elija correctamente al dispositivo que será la raíz, los equipos de la LAN darán un salto más.

Para este esquema se utilizará RSTP que ofrece una mayor rapidez de convergencia ante cualquier cambio en la topología de la red. Es más, la configuración de la característica *portfast* para los puertos de acceso, para que estos pasen del estado de bloqueo al estado de envío de manera automática.

En las siguientes líneas de comando que se mostrarán a continuación se han ejecutado en un Switch Cisco WS-C2960S de 24 puertos GigaEthernet. De manera predeterminada los switches tienen habilitado STP IEEE 802.1D; sin embargo, para habilitar RSTP se hará sobre la estancia de STP de Cisco llamada PVST (Per VLAN Spanning-Tree Protocol).

```
spanning-tree mode rapid-pvst[8]
```

Todos los switches en la red deberán ser configurados con la misma línea; sin embargo, en el caso de que no se haya realizado la configuración en alguno de los dispositivos, PVST+ rápido es compatible con STP (IEEE 801.2D) ya que está basado en el estándar 802.1w (RSTP).

En esta propuesta de red LAN existen tres VLAN en la red con los ID 100, 200 y 300. Los switches SW1, SW2, SW3 y SW4 están conectados entre sin con enlaces redundantes. Estos son FastEthernet.

Para garantizar que el Switch SW1 conectado al Router de salida sea el puente raíz, la modificación de la prioridad para todas las VLAN de la red es trascendental.

```
spanning-tree vlan 1-1005 priority 24576
```

De esta manera el Switch SW1 será tomado como referencia para toda la red en el cálculo de los caminos redundantes y la determinación del bloqueo de puertos y lograr el objetivo de evitar loops. El comando anterior determina que el Switch tendrá la prioridad de 24576 para el rango de VLAN entre 1 y 1005. Esa prioridad es más baja que la predeterminada de 32768 que no se cambiará para garantizar que el Switch SW1 será puente raíz.

Asimismo, en la topología de la 2.21 el Switch SW3 con sólo dos de sus puertos activados. Esto es para garantizar el camino entre el Switch SW1 y los switches los equipos de la VLAN 200. Para obtener ese resultado, SW3 debe tener un valor de prioridad mayor qué los switches SW2 y SW4 durante el proceso de elección de los roles para los puertos del segmento. La línea de configuración para obtener dicho resultado es el siguiente:

```
spanning-tree vlan 1-1005 priority 41060
```

Las interfaces hacia los switches que tienen un solo enlace automáticamente estarán en estado de envío (forwarding).

Para los switches SW2 y SW4 la elección del puerto raíz y el puerto alternativo (de respaldo) se basará primordialmente en la prioridad del puerto. La prioridad que tiene cada puerto es la de 128 de manera predeterminada más el número de interfaz que representa en el dispositivo. Por tal motivo, las primeras interfaces en un enlace redundante serán seleccionadas como interfaces de forwarding mientras que las otras entrarán en el estado de alternativo (o de respaldo) con el puerto bloqueado (discarding).

A continuación se presenta una parte de la salida del comando show spanning-tree ejecutado en el puente raíz para la VLAN 100.

[8] Las configuraciones mostradas para los switches de la red local son para un dispositivo Cisco® Catalyst WS-C2960S sobre sistema operativo Cisco IOS versión 15.0.

```
SW1#show spanning-tree vlan 100
VLAN0100
  Spanning tree enabled protocol rstp
  Root ID     Priority    24676
              Address     000A.4115.D7D8
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24676  (priority 24576 sys-id-ext 100)
              Address     000A.4115.D7D8
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/6            Desg FWD 19        128.6    P2p
Fa0/7            Desg FWD 19        128.7    P2p
```

Se puede observar que el Switch está habilitado para utilizar el protocolo RSTP, una prioridad más baja que la predeterminada permite que este sea el puente raíz de la red. Del mismo modo, los siete puertos troncales del Switch están en el estado de envío (forwarding) y con el rol de puerto designado. En la columna *Type* que aparece enseguida de la de prioridad de interfaces se muestra para cada puerto "*P2p*", esto se refiere al tipo de enlace, será punto a punto cuando se trata de una conexión entre dos switches con interfaces en modo *full* dúplex. También existe el enlace compartido hecha entre switches y hubs a través de una comunicación *half* dúplex.

La salida del mismo comando para el Switch SW3 es la siguiente:

```
SW3#show spanning-tree vlan 100
VLAN0100
  Spanning tree enabled protocol rstp
  Root ID     Priority    24676
              Address     000A.4115.D7D8
              Cost        19
              Port        1(FastEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    41060  (priority 40960 sys-id-ext 100)
              Address     00D0.5855.D311
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p
Fa0/3            Altn BLK 19        128.3    P2p
Fa0/4            Altn BLK 19        128.4    P2p
Fa0/5            Altn BLK 19        128.5    P2p
Fa0/6            Altn BLK 19        128.6    P2p
Fa0/7            Desg FWD 19        128.7    P2p
```

En este despliegue del comando, se puede notar que también está trabajando el protocolo de RSTP y su prioridad no es la predeterminada sino el valor de 41060. Todos los puertos se encuentran en estado de bloqueo (blocking)

tomando el rol de puertos alternativos (el puerto Fa0/2 es la interfaz de respaldo y se puede detectar fácilmente viendo el diagrama gráfico, este se encuentra cerca al puente raíz al igual que el enlace en Fa0/1).

Cualquier puerto de acceso será un puerto extremo. Para cerciorarse que este tipo de puertos tendrán una transición del estado de bloqueo al estado de enviar de manera automática, se configurará la sentencia de *portfast* en la interfaz.

Considerando que el puerto FastEthernet en el Switch SW3 es un puerto de acceso configurado en la VLAN 200, la configuración de portfast será de la siguiente manera:

```
SW3(config)#interface FastEthernet0/11
SW3(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/11 but will only
have effect when the interface is in a non-trunking mode.
SW3(config-if)#end
SW3#
```

Al configurarse el sistema operativo del dispositivo envía un mensaje de advertencia recordando al admnistrador que la configuración de portfast en una interfaz a un dispositivo de capa 2 podría causar loops en la red de manera temporal.

El puerto se habilitará al estado de envío sólo para la VLAN a la que s e encuentra configurado de acceso.

```
SW3#show spanning-tree interface FastEthernet 0/11 portfast
VLAN0001         enabled
VLAN0100         disabled
VLAN0200         enabled
VLAN0300         disabled
SW3#
```

Un aspecto importante antes del diseño de la red local es mantener el diámetro de la red a siete, es decir, para un host en la red, como máximo para llegar a otro en la misma red local como máximo debe transportarse a través de siete switches.

3

Seguridad de la red de datos

3.1 Implementación de la seguridad

La gestión de la seguridad de una red de datos es importante para mantener la disponibilidad, la confidencialidad e integridad de la información que circula en la red, y de los datos que son almacenados en equipos personales, así como de bases de datos. La información de las organizaciones es el activo más importarte de éstas, la pérdida de información sensible puede garantizar la pérdida de otro activo, el dinero, provocando incluso que la empresa o institución gubernamental o educativa deje de existir o sea víctima de graves consecuencias.

Asimismo, además de mantener la información de la organización segura, es importante poder garantizar que la red no esté siendo vulnerada por otras organizaciones, principalmente atacando a los dispositivos importantes en la red, como Routers, los cuales tienen la tarea de enrutar paquetes generados en la red local hacía internet. Del mismo modo, la manipulación de dispositivos de la red local por personas ajenas a las organizaciones para cualquier fin ilícito que afecte a la organización, ya sea a través de virus informáticos o acceso no autorizado a los equipos a través de conexiones remotas, debe de ser detectado por sistemas de seguridad en la red para que se generen alarmas que monitoreen los administradores, y estos sean capaces de eliminar las amenazas cerrando conexiones, o aislando a los equipos afectados de la red.

En lo que se refiere al tipo de datos que circularán en la red, y el tipo de información que puede ser consultada de las redes locales a internet, es de suma importancia tener control sobre los sitios que se visitan, evitando que se haga uso indebido de la red y de la información generada en la misma. El acceso a páginas web indebidas puede provocar que haya infección por virus informáticos de los equipos utilizados y desde ellos afectar a la organización. Por lo que respecta a la política de seguridad de la organización, es importante que la navegación de los usuarios las respete, los sitios permitidos variarán según el tipo de organización que se trate.

3.2 Firewalls sobre OpenBSD

Los Routers pfSense pueden ser configurados para ser administrados remotamente a través de SSH. De manera predeterminada, pfSense no tiene funcionando el servicio de SSH; sin embargo, este puede ser habilitado a través de la opción 14 del menú en la interfaz de línea de comandos. Figura 3.1

```
 7) Ping host

Enter an option: 14

SSHD is currently disabled.  Would you like to enable? [y/n]? y

Writing configuration... done.

Enabling SSHD... done.
```

Figura 3.51 Habilitando SSH en pfSense

De esta manera, desde las oficinas centrales se podrá administrar cada uno de los Routers de los planteles gracias a la gestión remota, siempre y cuando no se pierda la conexión con el dispositivo. Sin embargo, el acceso al puerto 22 del servicio habilitado está disponible a todos los dispositivos conectados en la red del IEMS. Esto último no es lo más viable, es una falla a la seguridad, estos dispositivos sólo deben ser accesibles a un grupo de usuarios específicos de la red, con ciertos privilegios, nombres de usuarios y contraseñas para lograr el ingreso a los dispositivos. Cada Router pfSense sólo será administrado vía SSH o HTTP por un conjunto de usuarios administradores en la red, por lo que es importante tener un firewall en todos los nodos.

Sólo los administradores de red deben de tener acceso a los Routers, así como es de importancia garantizar que sólo algunos servicios estén disponibles para los usuarios comunes, por ejemplo, sólo permitir el acceso web y de

correo, es decir, la red permitirá la salida de peticiones a los servicios de HTTP, HTTPS y SMTP, identificados por los puertos 80, 443 y 25.

Para lograr lo expuesto anteriormente, se puede hacer el uso de los firewalls en las que se indicarán ciertas reglas para permitir y denegar servicios a Internet y hacia dentro de la red y los dispositivos de la red. Cada uno de los nodos de la red del IEMS tendrá conectado a su salida un firewall, mismo que hará el filtrado de paquetes tanto en la descarga como en la carga de información. Sin embargo, esta tarea puede ser confiada al Router-on-a-stick que une a todos los planteles del IEMS y les da salida a internet. De esta manera, se pude determinar que los firewalls serán utilizados sólo para la protección de la gestión de los Routers pfSense y no para el control de los servicios a las redes locales.

El firewall será implementado bajo OpenBSD debido a que se trata de una herramienta de uso libre que ofrece gran funcionalidad y flexibilidad. Asimismo, se trata del sistema operativo más confiable actualmente.

La funcionalidad en la que se utilizará el firewall será en *modo transparente*. Un dispositivo en modo transparente es utilizado cuando se desea que el firewall no pueda ser identificado desde redes externas, ya que entre sus características, estos dispositivos no tienen una dirección IP en ninguna de sus interfaces, son transparentes al usuario; sin embargo, el firewall está en funcionamiento entre las dos redes, filtra los paquetes, y según las reglas que se hayan configurado en él, serán rechazadas u aprobadas las peticiones.

3.2.1 Instalación de OpenBSD

Se propone a OpenBSD como equipo para función de firewall de la red por su gran funcionalidad. La versión del OpenBSD que se instalará será la última que aparezca en el portal del sistema operativo *http://www.openbsd.org/*. El firewall OpenBSD va a ser utilizado en las dos modalidades en la red, ya sea en modo transparente o en modo público, siendo la última cuando se utilizará como dispositivo de reenvío de paquetes (Router) ya que es necesario que se tengan direcciones IP.

```
Choose your keyboard layout ('?' or 'L' for list) [default] la
kbd: keyboard mapping set to la
System hostname? (short form, e.g. 'foo') firewall_
```

Figura 3.52 Elección de distribución de teclado y nombre de equipo

Entre los aspectos importantes que se tienen que tomar en cuenta para la instalación de este sistema operativo con respecto a las necesidades de la red del IEMS, hay que elegir el nombre del sistema (figura 3.2), región horaria particionado del disco duro (este dependerá de la capacidad establecida, asignar espacio al directorio raíz, a /usr y a /var), y durante la selección de los paquetes a instalar, deseleccionar aquellos paquetes correspondientes al el entorno gráfico ni la instalación de juegos, procedidos por una "x" en el nombre para los gráficos, y un "game" para los juegos, tal como se puede observar en la figura 3.3.

```
Set name(s)? (or 'abort' or 'done') [done] -x*
    [X] bsd           [X] etc52.tgz     [ ] xbase52.tgz   [ ] xserv52.tgz
    [X] bsd.rd        [X] comp52.tgz    [ ] xetc52.tgz
    [ ] bsd.mp        [X] man52.tgz     [ ] xshare52.tgz
    [X] base52.tgz    [X] game52.tgz    [ ] xfont52.tgz
Set name(s)? (or 'abort' or 'done') [done] -gam*
    [X] bsd           [X] etc52.tgz     [ ] xbase52.tgz   [ ] xserv52.tgz
    [X] bsd.rd        [X] comp52.tgz    [ ] xetc52.tgz
    [ ] bsd.mp        [X] man52.tgz     [ ] xshare52.tgz
    [X] base52.tgz    [ ] game52.tgz    [ ] xfont52.tgz
Set name(s)? (or 'abort' or 'done') [done] _
```

Figura 3.53 Elección de paquetes a instalar.

Después de haberse realizado la selección de los paquetes a instalar, se ingresa un "*enter*" para que se haga la instalación de los mismos, finalizando con la instalación del OpenBSD, se requiere un reinicio, figura 3.4.

```
bsd           100% |*************************************|  8810 KB    00:11
bsd.rd        100% |*************************************|  6271 KB    00:09
base52.tgz    100% |*************************************| 55415 KB    02:12
etc52.tgz     100% |*************************************|   519 KB    00:01
comp52.tgz    100% |*************************************| 60165 KB    02:08
man52.tgz     100% |*************************************|  9497 KB    00:27
Location of sets? (cd disk ftp http or 'done') [done]
Time appears wrong.  Set to 'Mon Apr  8 13:54:44 CDT 2013'? [yes]
Saving configuration files...done.
Generating initial host.random file...done.
Making all device nodes...done.

CONGRATULATIONS! Your OpenBSD install has been successfully completed!
To boot the new system, enter 'reboot' at the command prompt.
When you login to your new system the first time, please read your mail
using the 'mail' command.

# _
```

Figura 3.54 Instalación de los paquetes de OpenBSD

3.2.2 Configuración del Firewall en modo *bridge* transparente

Los dispositivos que se utilizarán con la funcionalidad de firewall serán colocados en el Router de salida de cada plantel, para la protección de cada uno de los nodos, así como para el control del flujo de tráfico hacia ciertos servicios. La configuración del firewall será en modo transparente, es decir, cada una de las interfaces con las que contará tendrán una dirección IP, sólo el equipo realizará el análisis del tráfico que cruce sobre él. De esta manera, cada firewall no podrá ser administrado externamente, sólo de manera local en el cuarto de telecomunicaciones de cada plantel

Dado lo anterior, se da por entendido que el dispositivo firewall deberá poseer dos tarjetas físicas de red, una para la conexión de la red local, y otra que irá conectada al resto de la red. La topología que se implementará en el IEMS se muestra en la figura3.5.

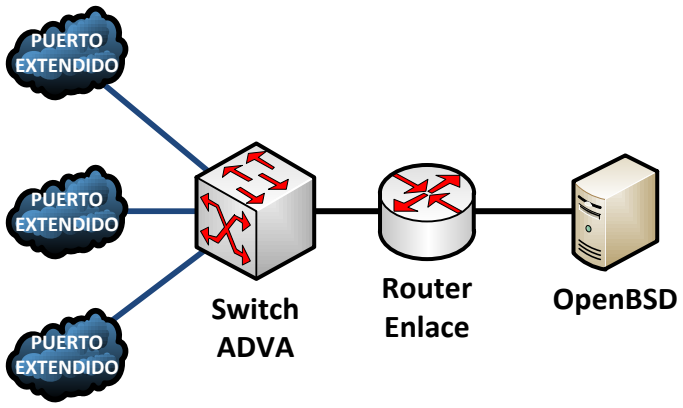

Figura 3.55. Ubicación de Firewall en la red del IEMS.

Como ya se mencionó anteriormente, la instalación de los firewall será bajo el sistema operativo OpenBSD, que además de ofrecer gran funcionalidad como dispositivo de seguridad de la red, es un sistema operativo bastante robusto, que utiliza muy bajos recursos de cómputo.

La versión de OpenBSD a instalar es la 5.2 que es la que actualmente se distribuye a través de su página oficial. Después de haber realizado la instalación de OpenBSD en el equipo, es necesaria la configuración del mismo. Una de las primeras configuraciones antes de establecer reglas de filtrado es la configuración del firewall en modo *bridge* transparente. Un bridge (puente) es un enlace entre dos o más redes separadas, y, con diferencia a un Router, los paquetes que son transferidos a través del *bridge* lo hacen "invisiblemente", los dos segmentos de red parecen ser uno a los nodos de cada lado del *bridge*. El *bridge* transmitirá únicamente los paquetes que tiene que pasar de un segmento a otro, por lo que, entre otras cosas, proveen una manera fácil de reducir el tráfico en una red compleja y permitir el acceso de un nodo a otro sólo cuando es necesario.

La configuración del firewall que se mostrará a continuación será el que estará colocado en el Plantel 9, por lo que las direcciones IP e imágenes mostradas corresponderán a los equipos instalados en el cuarto de telecomunicaciones de dicho nodo.

Antes de configurar el firewall en modo *bridge transparente*, es necesaria la identificación de las dos tarjetas de red a utilizar en el proceso, ya que es importante conocer cuál será la interfaz que conectará a la red local (interfaz interna) y cuál al resto de la red (interfaz externa), ya que en el proceso de desarrollo de las reglas de filtrado, su identificación por medio de macros será fundamental.

```
# ifconfig
vic0: flags=8802<BROADCAST,SIMPLEX,MULTICAST> mtu 1500
        lladdr 00:0c:29:90:c1:98
        priority: 0
        media: Ethernet autoselect
        status: no carrier
vic1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> mtu 1500
        lladdr 00:0c:29:90:c1:a2
        priority: 0
        media: Ethernet autoselect
        status: no carrier
```

Figura 3..56. Despliegue de información de interfaces por medio del comando IFCONFIG.

El equipo que se configurará y se mostrará en esta sección, la interfaz "vic0" es la interfaz conectada al enlace Lan-to-Lan, mientras que la interfaz "vic1" estará conectada a la interfaz del Router pfSense.

Identificadas las interfaces, se procede a la configuración de las interfaces. Ambas interfaces físicas en el firewall cuentan con un archivo que guarda la configuración de la misma, como dirección IP, o en su caso, sólo la activación lógica de la misma. Ese archivo es identificado como ***hostname.<nombre de la interfaz>*** ubicado en el directorio UNIX /etc. El firewall utilizado para la explicación en esta sección del capítulo deberá contar con los archivos hostname.vic0 y hostname.vic1. Estos archivos no existirán en el caso de que el equipo sea utilizado por primera vez sin ninguna configuración de red, de este modo, se deberán crear.

Los dos archivos deberán tener la siguiente línea: *media autoselect up*, misma que sólo seleccionará a la interfaz y las encenderá lógicamente (figura 3.7). Después de haber realizado lo anterior, se debe reiniciar el equipo.

```
/etc/hostname.vic1: new file: 1 lines, 20 characters
# cat /etc/hostname.vic
cat: /etc/hostname.vic: No such file or directory
# cat /etc/hostname.vic0
media autoselect up
# cat /etc/hostname.vic1
media autoselect up
# reboot_
```

Figura 3.57. Configuración de las interfaces por medio de sus archivos.

En la imagen anterior, sólo se despliega la información que ha sido guardada en los archivos correspondientes por medio del comando de UNIX *cat*.

Después de haber reiniciado el dispositivo y conectado el dispositivo físicamente a la red, se verifica que las interfaces hayan encendido, por medio del comando *ifconfig*, que deberá desplegar el dato de *status* de las interfaces como "active", figura 3.8.

```
# ifconfig
vic0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        lladdr 00:0c:29:90:c1:98
        priority: 0
        media: Ethernet autoselect
        status: active
        inet6 fe80::20c:29ff:fe90:c198%vic0 prefixlen 64 scopeid 0x1
vic1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        lladdr 00:0c:29:90:c1:a2
        priority: 0
        media: Ethernet autoselect
        status: active
        inet6 fe80::20c:29ff:fe90:c1a2%vic1 prefixlen 64 scopeid 0x2
```

Figura 3.58. Verificación del estado de las interfaces.

Una vez que las interfaces del firewall se encuentren activas, se procede a crear el *bridge*, creando un archivo llamado *hostname.bridge0* que integrará a las dos interfaces físicas del dispositivo en una sola lógicamente. Esto se realizará por medio de la instrucción *add vic0 add vic1 up* en el archivo (figura 3.9). La instrucción indicará al dispositivo que las interfaces del firewall estarán integradas en una misma, además de encender el bridge lógicamente.

```
# cat /etc/hostname.bridge0
add vic0 add vic1 up
# _
```

Figura 3.59. Configuración de la interfaz bridge.

Ya que configurado el bridge, es necesario realizar cambios en algunos parámetros para que funcione el firewall. Uno de los cambios a realizar se hará en el archivo */etc/sysctl.conf* en el que se modifica la línea *#net.inet.ip.forwarding=1* a *net.inet.ip.forwarding=1*quitando el símbolo de comentario '#', figura 3.10.

La modificación anterior es necesaria para permitirle al dispositivo que reenvíe el tráfico que fluya a través del él. Si no se realiza esta modificación, el tráfico de datos de un segmento de red a otro no se podrá llevar a cabo.

```
#
net.inet.ip.forwarding=1        # 1=Permit forwarding (routing) of IPv4 packets
```

Figura 3.60. Se habilita la capacidad de reenvío de paquetes a firewall.

Asimismo, es necesario que se ingrese al archivo */etc/rc.conf* y verificar que la línea de configuración del filtro de paquetes (PF) esté habilitada por medio de un YES en la línea correspondiente, de no ser así, se debe establecer así. Esta modificación es necesaria para habilitar en el firewall el funcionamiento del filtro de paquetes, este hará uso de las reglas que se establezcan para permitir o denegar cierto tipo de tráfico generado de la red hacía el exterior y viceversa. Figura 3.11.

```
pf=YES                          # Packet filter / NAT
```

Figura 3.61. Habilitación del filtro de paquetes.

Después de haber realizado las modificaciones correspondientes, es preciso realizar nuevamente el reinicio del dispositivo.

Una vez reiniciado el sistema, se verifica que se ha creado el bridge por medio del comando *ifconfig*, y que las dos interfaces físicas están relacionadas en él, figura 3.12.

```
bridge0: flags=41<UP,RUNNING>
        groups: bridge
        priority 32768 hellotime 2 fwddelay 15 maxage 20 holdcnt 6 proto rstp
        vic1 flags=3<LEARNING,DISCOVER>
                port 2 ifpriority 0 ifcost 0
        vic0 flags=3<LEARNING,DISCOVER>
                port 1 ifpriority 0 ifcost 0
```

Figura 3.62. Puente creado en el firewall.

Realizado esto, el bridge deberá dejar pasar todo tipo de tráfico. El Router pfSense debe de tener comunicación con su extremo en el enlace L2L a través del firewall OpenBSD. Esto se podrá verificar utilizando dos herramientas de diagnóstico, *ping* y *tcpdump*. Estas herramientas se encuentran en la mayoría de los sistemas operativos. Una de estas ya ha sido mencionada anteriormente en este trabajo: *ping*, la cual es utilizada para saber si una red es alcanzable desde otra desplegando estadísticas acerca de pérdidas y tiempos de llegada. *tcpdump* analiza los paquetes intercambiados entre hosts a través de la red. *tcpdump* es un analizador de protocolos que examina el contenido de los paquetes, incluyendo sus cabeceras. De esta manera, ping será utilizado enviando paquetes desde la red local del Plantel 9 a la interfaz virtual en el extremo del enlace L2L, a la dirección 172.16.30.35, mientras que el analizador de protocolos con *tcpdump* se activará en el firewall y se analizará el flujo del tráfico en el mismo para verificación del funcionamiento del bridge transparente, figura 3.14.

```
# tcpdump -i vic0 icmp
tcpdump: listening on vic0, link-type EN10MB
14:37:03.793838 10.30.30.34 > 10.30.30.33: icmp: echo request
14:37:03.795980 10.30.30.33 > 10.30.30.34: icmp: echo reply
14:37:04.676220 10.30.30.34 > 10.30.30.33: icmp: echo request
14:37:04.676256 10.30.30.33 > 10.30.30.34: icmp: echo reply
14:37:04.764769 10.30.30.34 > 10.30.30.33: icmp: echo request
14:37:04.771289 10.30.30.33 > 10.30.30.34: icmp: echo reply
14:37:05.669510 10.30.30.34 > 10.30.30.33: icmp: echo request
14:37:05.673499 10.30.30.33 > 10.30.30.34: icmp: echo reply
14:37:05.733698 10.30.30.34 > 10.30.30.33: icmp: echo request
14:37:05.814165 10.30.30.33 > 10.30.30.34: icmp: echo reply
14:37:06.677871 10.30.30.34 > 10.30.30.33: icmp: echo request
14:37:06.680117 10.30.30.33 > 10.30.30.34: icmp: echo reply
14:37:06.855287 10.30.30.34 > 10.30.30.33: icmp: echo request
14:37:06.857387 10.30.30.33 > 10.30.30.34: icmp: echo reply
^C
22 packets received by filter
0 packets dropped by kernel
# _
```

Figura 3.63. Análisis de tráfico en el firewall.

Después de haber iniciado un *ping extendido* desde algún host de la red local, se inicia el análisis de tráfico en la interfaz externa del firewall por medio del comando *tcpdump –i vic0 icmp*, donde se indica que los paquetes que deben ser analizados son los que cruzan sobre la interfaz vic0, delimitando también que sólo se analizará el tráfico del protocolo ICMP (Protocolo de Control de Mensajes de Internet) utilizado por la aplicación ping.

Se observa que el firewall en modo bridge ya está funcionando, las peticiones (request) de ICMP originadas desde la red local están siendo respondidas (reply) por la interfaz virtual al otro extremo del enlace Lan-to-Lan. Si se presta atención, se puede notar que no aparecen direcciones del segmento 172.16.9.0 de la red local aunque los paquetes de ping se originen de él. Esto es debido a que los paquetes están siendo reenviados por el Router pfSense a la salida, y por tal, aparece la dirección IP de su interfaz WAN.

A continuación se establecerán las reglas a utilizar para el filtrado de paquetes, mismas que seguirán una política de seguridad que cumpla con las actividades realizadas en el IEMS.

3.2.3 Estableciendo las reglas del filtrado de paquetes

Las reglas de filtrado que se establecerán son bastante simples. Se debe permitir el acceso al firewall pfSense por medio del puerto 443 y 22 para administración web y por medio de Secure Shell sólo a los administradores de la red. De manera predeterminada, el servicio de administración web de pfSense es por medio del protocolo HTTP (puerto 80); sin embargo, para mantener un esquema más seguro, se ingresará al dispositivo, y en el menú *System→Advanced*, en la sección llamada webConfigurator, se cambiará la opción seleccionada HTTP por HTTPS, figura 3.15.

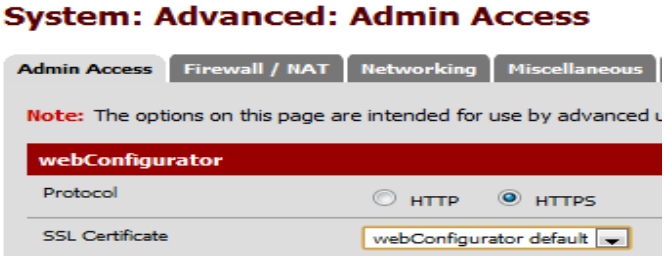

Figura 3.64. Habilitando HTTPS en el Router pfSense.

Al salvarse la nueva configuración, se desplegará un mensaje informando que se redirigirá a la página web utilizando el protocolo HTTPS. HTTPS o también conocido como HTTP Seguro provee autenticación de los sitios web para evitar los ataques de *hombre en medio*, asimismo, la transmisión de datos será cifrado.

Para cada red local hay un grupo de direcciones IP que pertenecen a dispositivos de los administradores de red. Por ejemplo, en el Plantel 9, las direcciones de red de los administradores comprende el rango de direcciones 172.16.9.104 a 172.16.9.111. Estás ocho direcciones pueden ser representadas por medio de una sola dirección y una máscara de subred que incluya dichas direcciones, tal como lo haría una máscara de Wildcard.

Las direcciones que se van a tomar en cuenta para la configuración del filtro de paquetes son las que se encuentran configuradas en la interfaz WAN de cada uno de los Routers pfSense.

Ese rango de direcciones se representaría por medio de la dirección 172.16.9.248 con la máscara 255.255.255.248, o prefijo /29. De esta manera, cada subred del IEMS cuenta con su grupo de usuarios administradores, todos en el mismo rango, por ejemplo, los administradores en la red del plantel Álvaro Obregón II están comprendidas en la dirección 172.16.2.248/29. La identificación de estas direcciones dentro de las subredes es importante para el establecimiento de las reglas de filtrado en los firewall. Estás reglas delimitarán que sólo un grupo de usuarios puedan acceder de manera remota a los firewalls a partir de la interfaz web o por medio de SSH.

Asimismo, es necesario el control de los servicios que se van a brindar a los usuarios locales. Los usuarios de las redes del IEMS sólo podrán utilizar los servicios de navegación web al puerto 80 y 443, así como servicios de correo electrónico, que utiliza el puerto 25 por medio del protocolo SMTP.

El filtro de paquetes, o conocido también como PF, es un sistema que filtra tráfico de TCP/IP y realiza Traducción de Direcciones de Red (NAT). PF es capaz de normalizar y condicionar el tráfico TCP/IP y proveer control del uso del ancho de banda y priorización de paquetes. La configuración del filtro de paquetes del firewall se realizará en el archivo */etc/pf.conf*.

Se procederá habilitando el filtrado de paquetes por medio del siguiente comando:

 # pfctl –e

PF lee las reglas configuradas del archivo */etc/pf.conf* durante el arranque. Es un archivo simple de texto que será interpretada por el filtro de paquetes.

La sintaxis general muy simplificada que se utilizará en este trabajo para las reglas de filtrado son las siguientes:

action [*direction*] [quick] [on *interface*] [proto *protocol*] [from *src_addr* [port *src_port*]]\
[to *dst_addr* [port *dst_port*]] [*state*]

Dónde:

- *action:* es la acción a seguir para los paquetes que tengan concordancia con la regla. Esa acción puede ser *pass* (dejas pasar) o *block* (denegar el paso). p*ass* dejará pasar el paquete hasta el núcleo del sistema para que este lo procese, mientras que *block* procesará el paquete según la política de bloqueo. La política de bloqueo (*block-policy*) puede determinar que el paquete sea eliminado (*block drop*) o se regrese al dispositivo un paquete TCP RST por paquete TCP bloqueado, o un paquete de *ICMP Unrecheable* (Inalcanzable) para el resto de los paquetes.
- *direction:* es la dirección a la que se moverá el paquete en la interfaz, ya sea *in* (entrante) u *out* (saliente).
- q*uick:* si el paquete concuerda con la regla que especifique *quick*, esta será considerada como la regla final para el paquete ejecutándose la acción sin la búsqueda de más reglas.
- *interface*: es el nombre de la interfaz en la cual el paquete se traslada.

- *protocol*: es el protocolo de capa cuatro del paquete, estos son: tcp, udp, icmp, icmp6, un número de protocolo entre 0 y 255.
- *src_addr*, *dst_addr*: es la dirección de origen y/o destino especificado en la cabecera IP. El valor se puede especificar como:
    - Una dirección IP versión 4 o versión 6.
    - Un bloque de red CIDR.
    - Un *Nombre de Dominio Totalmente Cualificado* (FQDN) que será resuelto por el DNS al cargarse las reglas, todo nombre será sustituido por su dirección IP.
    - Nombre de la interfaz. La dirección IP será sustituida en la regla.
    - Nombre de la interfaz seguido de la máscara de subred de si dirección IP por medio de prefijo CIDR.
- s*rc_port*, *dst_port*: el Puerto de origen y/o destino de capa 4 detallado en la cabecera IP. Este puede ser:
    - Un valor entre 1 y 65535.
    - Un grupo de puertos descrito en un alista.
    - Un rango de puertos.
- *state*: especifica si se guarda el estado de los paquetes que hayan concordado con la regla, se puede detallar lo siguiente:
    - *no state*: funciona con TCP, UDP e ICMP. No guarda el camino de la conexión.
    - *keep state*: es la regla predeterminada en todas las reglas. Se traza la conexión realizada por cada paquete.
    - *modulate state*: funciona sólo con TCP. PF genera números de secuencia para los paquetes que concuerden con la regla.

El uso de macros y buena utilización de las opciones de las reglas hacen que la edición del archivo y entendimiento sea sencillo, así como, las funciones de seguridad que brinda el dispositivo cumplirá con las políticas de seguridad específicas. La configuración del filtro de paquetes para uno de los planteles es el siguiente, utilizando las opciones descritas acerca de la sintaxis de las reglas para el filtrado de paquetes.

```
# cat /etc/pf.conf
EXT="vic0"
INT="vic1"
NET="10.30.30.34"

block all

pass in on $INT from $NET

pass out quick on $EXT proto icmp from any to any keep state

pass out quick on $EXT proto udp from any to any port 53 keep state

pass out quick on $EXT proto tcp from $NET to any port {www https} keep state
# _
```

Figura 3.65. Reglas de filtrado para el firewall en plantel 9

En la figura 3.16 se muestran las reglas de filtrado que se utilizarían en caso de que el control de los servicios de la red local estuvieran a cargo del firewall que está al borde de cada red LAN de los planteles. Se muestra que se han utilizado tres macros, dos para referencias a las interfaces del firewall, y otra para hacer relación a la dirección IP de la interfaz WAN del Router pfSense. Como ya se había mencionado anteriormente, la interfaz interna es aquella que está conectada a la interfaz WAN del Router, nombrada *vic1* en el sistema y que se manejará como "INT" en las reglas del filtro de paquetes, mientras que el extremo del enlace Lan-to-Lan se encuentra conectado a la interfaz *vic0* del firewall, llamada "EXT" en el archivo de configuración *pf.conf*. La macro "NET" guarda el valor de la dirección IP de la interfaz WAN del Router, esto es debido a que los paquetes generados en la red local tomarán la dirección

IP de su siguiente salto durante la comunicación, en este caso, la dirección IP de la interfaz WAN de su Router de salida.

La primera línea del archivo de configuración es "*block all*", en la que se indica que se bloquee todo el tráfico de manera predeterminada, de entrada y salida en el firewall, sólo se irá permitiendo el tráfico deseado.

La regla "*pass in on $INT from $NET*" permite que todo el tráfico saliente del Router pfSense entre al firewall a través de la interfaz *vic1*, referenciada como "INT". Este tráfico fue concebido en la red local, pero ha tomado la dirección IP de la interfaz WAN del Router, ya que fue el último salto que dio en su recorrido, por tal razón, se considera como fuente a la dirección IP 130.30.30.34. Este tráfico ha entrado al firewall, ahora se debe de determinar cuáles son los paquetes que saldrán del dispositivo.

La siguiente regla "*pass out quick on $EXT proto icmp from any to any keep state*" indica que los paquetes generados en la red local y en el Router por envíos de ping saldrán del firewall a través de la interfaz de salida *vic0*, que está referenciada por medio de la macro "EXT". Esto permitirá que cuando se ejecute un PING (uso del protocolo ICMP) en la red local para prueba de conectividad en la red será permitido. En esta regla no se indicó el origen, se utilizó la sentencia "any" para establecer que cualquier fuente; sin embargo, de cualquier modo, la dirección origen siempre será la dirección IP de la interfaz WAN. Se pudo haber colocado la regla como *pass out quick on $EXT proto icmp from $NET to any keep state*" y se tendría el mismo efecto en este caso.

En lo que se refiere a la regla "*pass out quick on $EXT proto udp from any to any port 53 keep state*", se mantiene la misma estructura que la regla anterior, sin embargo, el protocolo utilizado es UDP para el servicio otorgado a través del puerto 53 utilizado para el Sistema de Nombre de Dominio (DNS). Esta regla es importante para la realización de traducciones de dirección IP a sus respectivos nombres de dominio y viceversa, ya sea en la navegación web o el envío de un simple paquete PING a un dominio, y no a una dirección IP. Todo tráfico generado por la red local para el servicio de DNS saldrá del firewall a través de su interfaz *vic0*.

```
[2.0.1-RELEASE][root@Plantel9.iems.edu.mx]/root(4): ping www.iems.df.gob.mx
PING iems.df.gob.mx (201.144.232.206): 56 data bytes
64 bytes from 201.144.232.206: icmp_seq=0 ttl=58 time=27.849 ms
64 bytes from 201.144.232.206: icmp_seq=1 ttl=58 time=25.757 ms
64 bytes from 201.144.232.206: icmp_seq=2 ttl=58 time=26.846 ms
64 bytes from 201.144.232.206: icmp_seq=3 ttl=58 time=25.666 ms
64 bytes from 201.144.232.206: icmp_seq=4 ttl=58 time=39.291 ms
^C
--- iems.df.gob.mx ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 25.666/29.082/39.291/5.167 ms
[2.0.1-RELEASE][root@Plantel9.iems.edu.mx]/root(5):
```

Figura 3.66. El tráfico hacia el servicio de DNS por ICMP.

La última regla descrita en el archivo de configuración del filtro de paquetes es la siguiente: "*pass out quick on $EXT proto udp from $NET to any port {www https} keep state*", que indica que se dejará salir del dispositivo el tráfico generado en la red interna hacia los servicios www (web http, por el puerto 80) y https (web seguro, por medio del puerto 443).

Todas las reglas tienen al final de las mismas el parámetro "*keep state*", mismo que pudo haber sido ignorado ya que de manera predeterminada todas las reglas lo implementan al no colocarse algún valor.

Para que las reglas configuradas en el archivo sean las que utiliza el filtro de paquetes, es necesaria la ejecución de un comando que lo garantice. Ese comando es "*pfctl –f /etc/pf.conf –o none –e*" que por medio de la opción "f" indica que se cargue el archivo "/etc/pf.conf", la opción "–o none" indica que no se utilizará el optimizador de

reglas, y la opción "-e" habilita el filtro de paquetes en caso de que esté deshabilitado. El comando indicará si las reglas tienen error en su sintaxis, así como el número de línea en la que se presentó.

Las reglas que están en operación en el sistema se pueden ver por medio del comando "*pfctl –sr*". De esta manera se puede comprobar que las reglas se han cargado satisfactoriamente (figura 3.18). Des mismo modo, se pueden ver las reglas desmenuzadas por servicio y las macros se han remplazado por sus valores específicos.

```
# pfctl -f /etc/pf.conf -o none -e
pfctl: pf already enabled
# pfctl -sr
block drop all
pass in on vic1 inet from 10.30.30.34 to any flags S/SA keep state
pass out quick on vic0 proto icmp all keep state
pass out quick on vic0 proto udp from any to any port = domain keep state
pass out quick on vic0 inet proto tcp from 10.30.30.34 to any port = www flags S
/SA keep state
pass out quick on vic0 inet proto tcp from 10.30.30.34 to any port = https flags
 S/SA keep state
# _
```

Figura 3.67. Carga de reglas y verificación de las mismas.

3.3 Control de la navegación en Internet

La seguridad de una red de datos en operación comienza por proteger y controlar el tipo de información y *sitios web* que visitan sus usuarios. Diversos sitios web utilizan temáticas atractivas a los usuarios de la red que utilizan Internet para estudio y trabajo. Estos sitios en diversas ocasiones utilizan dicho camino para poder infectar a los cibernautas por medio de virus informáticos, mismos que se propagan a través de todos los equipos de una red y pueden causar estragos importantes en el desempeño de la red y denegar el servicio a sus clientes.

De la misma manera, es importante que organizaciones educativas y empresariales tengan la confianza de que los usuarios que utilizan su red están visualizando en sus dispositivos contenido apropiado que no afecte a sus actividades cotidianas y se encuentren enfocadas a su área de trabajo o a favor de su desarrollo. Sin embargo, cada una de las organizaciones tendrá ciertas páginas web permitidas y otras no, todo depende de la política de seguridad establecida en la empresa.

Por tal razón se hace uso de filtros de contenido que tienen como principales funciones las siguientes:

- Denegación de algunos servicios de Internet.
- Bloqueo de información que sale de la red. Esta característica es importante para proteger que información sensible dentro de la organización salga de ella, así como datos personales de sus integrantes.
- Limitación del tiempo de navegación de los usuarios. Se especifican tiempos y horarios determinados en la que los usuarios pueden hacer uso de Internet.
- Se permite crear perfiles de usuarios, algunos tienen más restricciones que otros.

Una de las herramientas que se propone a utilizar para realizar el filtrado de contenido del IEMS será un será un *Proxy*. Un proxy es un programa que puede ser instalado como un servidor sobre cualquier sistema operativo, o puede ser una aplicación. La modalidad que se utilizará en la red del IEMS es como servidor, sobre un sistema operativo Linux, y será ubicado al borde de la red.

Los usos que tiene un servidor proxy son las siguientes:

- Mantiene a los hosts de la red detrás de él anónimos, principalmente por seguridad.

- Proporciona gran velocidad de acceso a los recursos de la red debido a que hace uso de su *memoria caché* en la que almacena los sitios más recurrentes por los usuarios, no es necesario hacer la petición hacia internet si la página no ha cambiado.
- Aplicar políticas de acceso a servicios de red o contenido, por ejemplo, bloqueo a páginas web no deseadas.
- Utiliza archivos para el registro de hechos que ocurren en la red, y poder ser utilizados en caso de una auditoría.
- Escaneo de información de entrada para la búsqueda de malware hacia la red.
- Escaneo de la información de salida para evitar la pérdida de datos.

Un proxy puede ser ubicado en la computadora del usuario como una aplicación más instalada en el sistema, o se puede ubicar un equipo que funcione como proxy de toda la red y por obvias razones se ubicará junto con los Routers de salida.

3.3.1 Usos de los servidores proxy

Un servidor proxy provee control administrativo sobre el contenido que puede ser retardado en una o ambas direcciones a través del proxy. Es comúnmente utilizado en organizaciones comerciales y no comerciales (cómo escuelas) para garantizar que el uso de Internet cumpla con las políticas de seguridad de la organización.

Un proxy de filtrado de contenido soportaría autenticación de usuarios y control de acceso web. Usualmente también genera archivos de registro que muestran información detallada acerca de las URL acosadas por usuarios específicos, o monitorizar el ancho de banda utilizado. También podría comunicar por medio de un demonio[9] al software de antivirus acerca de amenazas como malware y actuar en contra de ellas en tiempo real antes de que actúen en la red.

Muchos lugares de trabajo, escuelas y colegios restringen sitios web y servicios en línea que están disponibles a todo público en la red. Esto puede ser realizado por medio de un proxy especializado, llamado también filtro de contenido.

Algunos métodos comunes usados para el filtrado de contenido incluye: creación de listas negras de URL y DNS. Los equipos dentro de la red ejecutan solicitudes web hacía Internet, mismas que pasan a través del proxy. El proxy es capaz de revisar la sintaxis de las URL y las asocia a su base de datos. Si hay coincidencia con alguna en la lista negra, la petición es rechazada y dependiendo el diseño del proxy, este le puede notificar al usuario que la página web que intentó ver está prohibida en la organización, o simplemente denegar el servicio.

Por otra parte, los servidores proxy aceleran el servicio a las respuestas de los clientes a Internet dado que cuentan con un sistema de memoria caché. Los proxy con caché guardan copias de los recursos de la red más visitados en memoria, permitiendo a las grandes organizaciones reducir significativamente el uso del ancho de banda y reducción de costos., mientras que se incrementa el desempeño.

Otro uso importante de un servidor proxy es la reducción del costo por hardware. Una organización puede tener muchos sistemas en la misma red o bajo el control de un servidor simple, prohibiendo la posibilidad de una conexión individual a Internet por cada sistema. En tal caso, los sistemas individuales pueden ser conectados a un servidor proxy, y el servidor proxy conectado al servidor principal.

[9] Es un tipo especial de proceso informático no interactivo, es decir, que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario. Este tipo de programas se ejecutan de forma continua (infinita), vale decir, que aunque se intente cerrar o matar el proceso, este continuará en ejecución o se reiniciará automáticamente. Todo esto sin intervención de terceros y sin dependencia de consola alguna.

3.3.2 Implementación de servidor proxy sobre *OPENBSD*

A continuación se presenta la implementación del servidor de filtrado de contenido sobre el sistema OpenBSD para su uso en la red Institucional que va desde los puntos clave como su ubicación en la red, instalación del sistema operativo y herramientas, tal como Squid y squidGuard, y por último, el establecimiento de las reglas de filtrado.

3.3.2.1 El sistema de filtrado de contenido del IEMS por medio de OPENBSD

En el IEMS como una organización educativa del gobierno del Distrito Federal, se vuelve importante garantizar que el uso de Internet por los usuarios de su red sea la correcta y que cumpla con los objetivos y misión de la institución educativa. Asimismo, los empleados del IEMS que utilizan la red de datos deben utilizar su infraestructura para usos de desarrollo, aprendizaje y compartir información relevante para el crecimiento de la institución, de los estudiantes y de ellos mismos, sin descuidar sus labores en su área de trabajo. Sin embargo, es importante mantener el control del uso de los recursos de Internet por los administradores de la red, y una de las principales tareas que se tienen es la implementación de un sistema que garantice que el contenido que se consulta en Internet es apto para las actividades llevadas a cabo dentro de la institución.

Debido a lo anterior, es importante que se lleve a cabo la implementación de un sistema de control de contenido en la red del IEMS. Con ello, Dansguardian se convierte en la opción más fiable a utilizar para esta tarea, ya que es una herramienta de uso libre y con características técnicas avanzadas que cumplen con las tareas que se cubrirán. De esta manera, Dansguardian se vuelve en una herramienta económicamente barata y funcional.

Como se habló en el capítulo anterior, la red que conforma al IEMS se basa principalmente en la utilización de puertos extendidos por medio de los enlaces LAN-to-LAN (L2L). Esta forma de conexión entre los nodos del IEMS permite que se no se utilice la red pública de Internet, sino un transporte privado que garantiza la seguridad del transporte de la información a través de la red interna. Sin embargo, la red ofrece un punto de salida a Internet a sus usuarios. La navegación hacia Internet por los usuarios del IEMS debe de ser controlada para evitar que se visiten sitios indebidos que afecten el desempeño en sus actividades escolares o laborales, así como evitar la infección de los equipos de cómputo por virus informáticos, por lo cual, es importante el uso de un sistema de filtrado de contenido como Dansguardian. El filtro de contenido se encontrará ubicado al borde de la red entre la salida a Internet y la red del IEMS.

Para que los *navegadores web* en los equipos de cómputo de los usuarios finales no se tengan que configurar con la dirección del servidor proxy, se utilizará una regla en el firewall del Router de pfSense de salida que redireccionará el tráfico de salida al proxy y este analizará el tráfico. El usuario final no verá el sitio no permitido debido a que la petición no será respondida por el servidor. Todo sitio que sea válido, se podrá visualizar sin problemas.

En la figura 3.19 se muestra la distribución y conexión física de los dispositivos al borde de la red del IEMS con el servidor proxy en funcionamiento. Existen dos opciones de conexión, una de ellas es en la que el Router de borde es el propio OpenBSD, en esta conexión, el firewall es visible en la red por contar con direccionamiento en las interfaces, pero el squid es transparente; sin embargo, la segunda opción de conexión es aquella en la que se cuenta con un Router de alguna marca comercial como salida, en este caso tanto el firewall como el squid son transparentes. Las configuraciones son las mismas, con excepción del firewall, este es sin direccionamiento y no existe la necesidad de hacer una traducción de direcciones de red de direccionamiento privado a público.

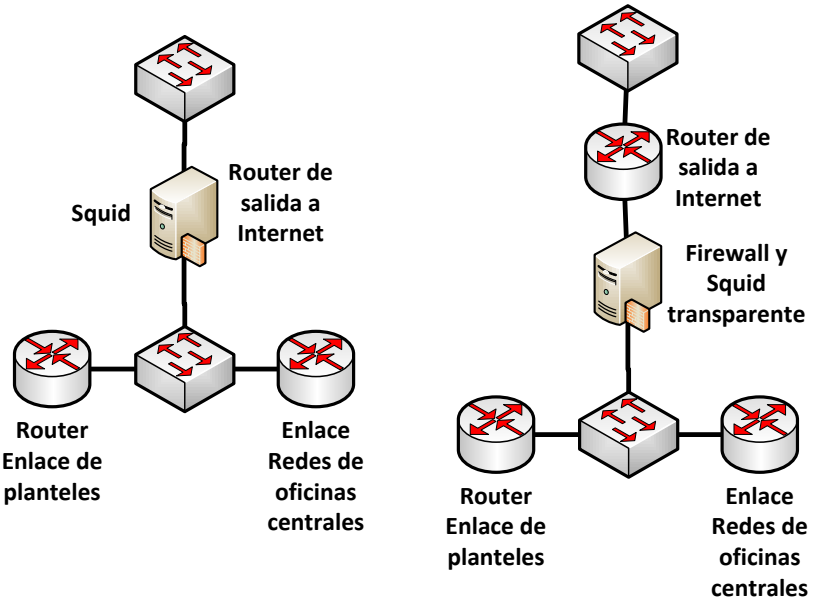

Figura 3.68. Ubicación del proxy en la red.

Las características que tiene el equipo que da salida a la red de Internet son las siguientes:

- OpenBSD está ejecutándose como Router de la red.
- Este mismo equipo está corriendo Packet Filter (Filtro de paquetes, pf).
- Este propio equipo trabaja con squid instalado trabajando como proxy transparente.
- El filtrado de paquetes está en línea, el acceso a Internet trabaja desde el Router y desde la red interna con squid trabajando transparentemente.

3.3.2.2 Instalación y configuración del Router OpenBSD

La instalación de OpenBSD es la misma que se mostró en el punto 3.1.1. Sin embargo, hay una línea importante que se añade a las reglas del Packet Filter, debido a que se trata de un Router que dará salida a las redes de la institución, este se encuentra conectado a Internet a través de un enlace, y por tal, el proveedor de servicios ha proporcionado una dirección IP pública. No obstante, con la configuración que se había detallado anteriormente, el dispositivo no ofrece salida a Internet, el tráfico sale de la red, pero en Internet este tráfico no puede ser enrutado debido a que se trata de direccionamiento privado.

Por tal razón, además de la restricción de los usuarios comunes a salir a direcciones de internet distintos de los puertos web, se implementará una regla que realice la Traducción de Direcciones de Red (NAT por sus siglas en inglés) de las redes privadas con las que se trabaja en la red interna.

```
EXT = "vic0"
INT = "vic1"
RED = "10.0.0.0/8 172.16.0.0/16"
ADMIN = "172.16.9.248/8"

block all
pass in on $INT from $RED
match out quick on $EXT from $RED to any nat-to $EXT
pass out quick on $EXT inet proto tcp from $EXT to any port {www https}
pass out quick on $EXT inet proto tcp from $ADMIN to any port
pass out quick on $EXT inet proto udp from $EXT to any port 53
pass out quick on $EXT inet proto icmp from any to any
```

De esta manera, a través de las reglas anteriores se garantiza que la red de la institución tenga salida a Internet por medio del comando *match out quick on $EXT from $RED to any nat-to $EXT* en la que se determina que todo el tráfico de la red interna que salga a través de la interfaz que está conectada a Internet será trasladado a la dirección de esa interfaz. Además, se ha definido una regla para el tráfico generado por los administradores de red que permite a su segmento de red una salida a Internet sin restricciones, esto a través de la línea *pass out quick on $EXT inet proto tcp from $ADMIN to any port*. Esta regla se puede replicar para los demás segmentos en las diferentes subredes o para hacer más estética y simple la presentación de las reglas, se puede modificar la macro ADMIN y agregar los segmentos de red de los administradores ubicados en las diferentes subredes de la red.

Además, es importante haber quitado el símbolo '#' en la línea *net.inet.ip.forwarding=1*para habilitar el ruteo en el dispositivo. Al realizar esta actividad, para que se tenga efecto se tiene que reiniciar el equipo.

De esta manera, ya se tiene instalado y configurado OpenBSD como un Router y está funcionando el Packet Filter sin problemas.

3.3.2.3 Squid y SquidGuard, instalación y configuración

Squid es un proxy caché que soporta los protocolos de HTTP, HTTPS, FTP y más para su filtrado. Si implementación reduce en la red el ancho de banda utilizado ya que debido a que los sitios más visitados se guardan en la memoria de caché, estos ya no tienen que ser descargados desde Internet para su visualización. Squid tiene n extensivo control de acceso y hace un servidor rápido. Este puede ser ejecutado en los sistemas operativos más populares, incluyendo Windows y aquellos bajo licencia GNU GPL (Licencia Pública General de GNU).

Squid es usado por miles de proveedores de Internet para brindar el mejor acceso web posible a sus usuarios. Squid optimiza el flujo de datos entre los usuarios y los servidores para mejorar el desempeño y almacena en caché el contenido más visitado.

Además, Squid será utilizado en conjunto con squidGuard. SquidGuard es un software de redirección de URL que es usado como control de acceso a contenido. Es escrito como un *plug-in*[10] de Squid y usa *listas negras* que definen qué sitios serán redirigidos. SquidGuard debe de ser instalado en un equipo de cómputo sobre el sistema operativo Unix o una variante de GNU/Linux con funciones de servidor. Este servicio se extenderá a todos los dispositivos de la red local sin importar el sistema operativo en el que funcionen.

SquidGuard es software libre que se distribuye bajo licencia GNU General Public License (GPL) y está incluido en muchas distribuciones de Linux como Debian, OpenSUSE y Ubuntu, además de varios sistemas Unix como es el caso de OpenBSD y FreeBSD.

[10] En computación, un plug-in es un componente de software que agrega características a una aplicación de software existente. Cuando una aplicación suporta plug.ins, esta habilita la personalización de la configuración.

Este servicio de filtrado de contenido será configurado en la red institucional para el control de la navegación de los usuarios. Es indispensable la creación de perfiles de usuarios, cada uno de estos tendrá diferentes permisos de navegación en Internet.

Este servicio será instalado y configurado en el equipo OpenBSD que da salida a Internet a toda la red del IEMS, es decir, en el equipo que está conectado a los enlaces de Internet. También puede ser configurado e instalado un servidor proxy en la salida de la red local de algún plantel. A continuación se da el proceso de instalación de los servicios necesarios para que el contenido de filtrado sea posible en esta red.

Este proceso de instalación y configuración esta hecho en su totalidad bajo la Interfaz de Línea de Comandos del equipo OpenBSD. Se agrega una ruta de descarga de paquetes por medio del comando *export*. Esta operación es necesaria para que los paquetes descargados sean instalados en el equipo. En la siguiente línea se escoge un servidor ubicado en Dallas, Texas, para la descarga de los paquetes ubicado geográficamente lo más cercano posible, esto para evitar lentitud en las descargas.

```
export PKG_PATH="http://mirror.esc7.net/pub/OpenBSD/5.2/packages/i386/"
```

Notar que la línea anterior considera a la arquitectura i386 de procesador Intel®[11], esta tendrá que ser la correspondiente al equipo que se esté utilizando en ese momento para que trabaje como servidor squid.

A continuación se procede a la instalación de Squid, será por medio del comando *pkg_add* de OpenBSD, que descarga el paquete que se le indique buscando en la ruta que se le haya establecido por medio del comando *export*.

```
# pkg_add -i squid
Ambiguous: choose package for squid
 a       0: <None>
         1: squid-2.7.STABLE9p19
         2: squid-2.7.STABLE9p19-ldap
         3: squid-2.7.STABLE9p19-ldap-snmp
         4: squid-2.7.STABLE9p19-ntlm
         5: squid-2.7.STABLE9p19-snmp
Your choice: 1
squid-2.7.STABLE9p19: ok
The following new rcscripts were installed: /etc/rc.d/squid
See rc.d(8) for details.
Look in /usr/local/share/doc/pkg-readmes for extra documentation.
#
```

Por medio del comando *pkg_add –i squid* se indica que se instale el paquete con nombre squid; sin embargo, en caso de que existan más de un paquete con el mismo nombre (por versiones de software), desplegará el paquete de "*Ambiguous*" tal como sucedió en la salioda de comando mostrada anteriormente. Se instalará el paquete 1 que permite la instalación de squid versión 2.7, las demás versiones permiten la autenticación, otras el envío de *traps* de SNMP para su monitorización.

Uno de los mensajes resultado de la instalación de Squid indica que se ha generado un nuevo script en el directorio /etc/rc.d/squid, esto indica que Squid puede ser invocado para su ejecución por medio del comando *squid* en OpenBSD.

[11] Intel es una corporación multinacional Americana fabricante de chips semiconductores ubicada en Santa Clara California. Inventor de la serie de microprocesadores x86.

Después de la instalación, es posible percatase que se han creado en el sistema los directorios correspondientes a squid, configuración y almacenamiento de datos. El archivo principal es el de configuración, se procede a editar algunos parámetros para el funcionamiento.

Se indicará el puerto de escucha del servicio de Squid, se dejará el puerto por default en modo transparente, esto es el funcionamiento que se desea en el plantel del IEMS para que para el usuario sea transparente en cuestión de configuración de parámetros en sus navegadores web[12].

```
http_port 3128 transparent
```

También es importante el establecimiento de la memoria caché. Debido a que se trata de una institución con alrededor de 3000 usuarios con salida a Internet, habrá una cantidad considerable de sitios web que serán visitados, pero muchos sitios web serán los mismos para la mayoría de los usuarios, por lo que el uso de la memoria caché es fundamental para evitar que las peticiones hacia Internet sean constantes (y evitar la saturación de los enlaces hacia Internet) y las respuestas a los usuarios sean más rápidas (ya no se tiene que salir hacia Internet para mostrar el contenido Web de un sitio en específico). Por esta razón, se establecerá una memoria de 2.5 Gigabytes de memoria de caché, pensando en un crecimiento de usuarios en los planteles. Si se tratase de un servidor en una red local con un promedio de 200 usuarios, con 100 Megabytes de memoria en la caché de proxy sería suficiente.

```
cache_dir ufs /var/squid/cache 2500 1000 256
```

La línea define que el directorio /va/squid/cache que se originó a la instalación de Squid se utilizará como sector de memoria caché para el proxy. Esta línea de manera predeterminada está comentada (por medio del carácter '#' para no tener efecto en la configuración por defecto), pero se des comenta para que tenga efecto e4n el proxy que se utilizará. Se define como un sector de memoria sobre el Sistema de Archivos Unix UFS (por sus siglas en inglés), con 2500 Megabytes de memoria (2.5 Gigabytes), y 1000 subdirectorios con 256 subdirectorios en cada uno.

Se especifica una dirección de correo electrónico que aparecerá en las páginas de error emitidas por el servidor en caso de denegarse alguna petición, esto en caso de que no se modifiquen las páginas de error que están de manera predeterminada en el servidor, por una personalizada.

```
cache_mgr <Dirección_de_correo_electrónico_administrador>
```

Se define el usuario y grupo efectivo que trabajarán con las peticiones de Squid y su almacenamiento en la memoria de caché, se establecerá el usuario y grupo que se crearon durante la instalación de Squid, el usuario _squid y el grupo _squid.

```
cache_effective_user    _squid
cache_effective_group   _squid
```

A continuación se definen los parámetros de configuración para los registros (archivos de log) que se generarán durante el funcionamiento de Squid.

```
logformat squid  %ts.%03tu %6tr %>a %Ss/%03Hs %<st %rm %ru %un %Sh/%<A %mt
access_log       /var/squid/logs/access.log squid
cache_log        /var/squid/logs/cache.log
cache_store_log  /var/squid/logs/store.log
```

[12] Un navegador web (comúnmente llamado navegador) es una aplicación de software utilizado para recuperar, presentar y compartir recursos de información en la World Wide Web. Estos recursos pueden ser desde páginas web, textos, imágenes, video, audio o cualquier otra pieza de contenido. Estre los navegadores web más utilizados están Google Chrome, Mozilla Firefox y Microsoft Internet Explorer.

La primera línea define el formato en la que se guardarán las entradas a los archivos de registro, es decir, la forma en que se mostrará la información que se almacena. La sentencia *access_log* define el archivo de en el que se guardarán las peticiones a sitios web de todos los usuarios. También se guardan los registros del comportamiento de la memoria caché y el administrados de almacenamiento por medio de las sentencias *cache_log* y *cache_store_log*.

Los dos parámetros que se colocarán en el archivo de configuración de Squid serán el nombre del dispositivo y el idioma en el que aparecerán los mensajes de error de conexión (en caso de quedarse las configuraciones por defecto).

```
visible_hostname PROXY_OPENBSD
error_directory /usr/local/share/squid/errors/Spanish
```

Como ejemplo, se configure como nombre del servidor *PROXY_OPENBSD*, y los mensajes de error que se muestren en español.

Probar que la sintaxis del archivo de configuración de Squid está correcto (por medio del comando squid y los argumento –f para indicar el archivo, y –k para indicar l acción), asimismo, ejecutarlo si no hay problema de sintaxis (squid –z para la creación de los directorio swap) y comprobar que el puerto 3128 se ha abierto y está en escucha (a través del comando *netstat*).

```
# squid -f /etc/squid/squid.conf -k parse
# squid -z
2013/04/15 01:44:02| Creating Swap Directories
# squid start
# netstat -an | grep 3128
tcp          0      0  *.3128                 *.*                    LISTEN
#
```

El comando squid por medio de los argumentos “-k purse” revisan la sintaxis del archivo de configuración, en caso de que exista un error, este comando alertará e indicará la el número de la línea que está causando el problema.

Ahora prosigue la instalación de SquidGuard, esta es más sencilla. Además de instalarse SquidGuard, también lo hará el gestor de base de datos de Berkeley (DB Berkeley) ya que es utilizado para su funcionamiento. Utilizando la misma ruta al sitio de Dallas para la descarga de paquetes, se instala SquidGuard a través del comando pkg_add:

```
# pkg_add -i squidGuard

Ambiguous: choose package for squidGuard
 a       0: <None>
         1: squidGuard-1.4p3
         2: squidGuard-1.4p3-ldap
Your choice: 1

 squidGuard-1.4p3:db-4.6.21v0: ok
squidGuard-1.4p3: ok
#
```

Debido a que existe más de un paquete con el mismo nombre, aparecerá el mensaje de “Ambiguo”, pero se desplegará una lista con las opciones disponibles, se elige la primera opción, la otra es cuando se utiliza autenticación.

De esta manera se tienen instaladas las herramientas necesarias para realizar el filtrado. En el siguiente punto se establece la configuración y establecimiento de las reglas de filtrado.

3.3.2.4 Establecimiento de reglas de filtrado de contenido

La configuración del archivo de Squid ya se trató en el punto anterior; sin embargo, se hará uso del plug-in SquidGuard para el establecimiento de las reglas de filtrado de contenido. Asimismo, el tráfico que se genera de la red local hacia el puerto web en sitios en Internet tendrá que ser redirigido al puerto 3128 del proxy para ser filtrado primero y después enviar al exterior.

La población de la red de la institución consta de estudiantes, profesores, empleados administrativos y de confianza, directivos y administradores de red. Estos últimos son los que administran el servidor proxy y los servicios de telecomunicaciones de la institución que tienen a su cargo.

El servidor proxy puede ser instalado en la salida de cada uno de los planteles, o en la conexión de toda la institución hacia Internet. Aquí se mostrará la de un plantel en específico; sin embargo, la configuración para utilizarse en un dispositivo al borde de la red es la misma, sólo con mayor información debido a que se deben de tomar en cuenta más segmentos de red y el significado que tienen en cada red local de plantel.

En este trabajo se ha trabajado con un direccionamiento con 254 equipos por red en cada plantel; sin embargo, esto es fácilmente modificable para tener un mayor número de hosts por plantel, no hay problema, pues el direccionamiento utilizado es público y para una Institución del tamaño del IEMS, ese espacio de direcciones es suficiente para su utilización.

A continuación se explicará la configuración de las reglas del filtrado con un ejemplo de requerimientos y de direccionamiento propuestos posible que se puede dar en la Institución educativa.

Se tienen para el plantel 9 un segmento de red 172.16.9.0/24, es decir, 254 direcciones de red útiles; para estas direcciones IP, las últimas 7 son para los equipos de los administradores de red, de la 172.16.9.248 a la 172.16.9.254. La dirección IP de la computadora del director del plantel y su suplente son la 172.16.9.247 172.16.9.246. Las direcciones IP de los dispositivos de los administrativos y empleados de confianza son 172.16.9.235 a la 172.16.9.245. Se cuenta con direccionamiento para los equipos de los profesores, son 15, se tiene el direccionamiento del 172.16.9.220 a la 172.16.9.234. El direccionamiento de impresoras, servicio y teléfonos son 172.16.9.210 y 172.16.9.219. El direccionamiento restante es centros de cómputo destinados a la enseñanza.

Con dicha información se puede establecer lo siguiente: Las direcciones de red asignadas a centros de cómputo para los alumnos tiene acceso limitado, sitios de pornografía, apuestas y juegos. Para administradores de red y directivo se tienen acceso libre, sin denegaciones a cualquier sitio a la red y se confiará que las personas en estos cargos utilicen los recursos de buena forma y encaminado al desarrollo de sus actividades, y por ende, el desarrollo de la Institución.

En la siguiente tabla se registra las reglas que se trasladarán a configuración para el filtrado por medio de Squid:

Tabla 3.1. Definición de perfiles de usuarios a partir de rangos de direcciones IP.

Rol en la Institución	Direccionamiento	Permisos y denegaciones
Directivos	172.16.9.247 y 172.16.9.246	Sin restricción
Administradores de red	172.16.9.248 - 172.16.9.254	Sin restricción
Personal de confianza	172.16.9.235 - 172.16.9.245	Ámbito laboral
Dispositivos dedicados	172.16.9.210 - 172.16.9.219	No salen a Internet, acceso local
Profesores	172.16.9.220 - 172.16.9.234	Ámbito laboral
Alumnos	172.16.9.1 172.16.9.209	Ámbito educativo

De esta manera es posible establecer la configuración de las reglas de filtrado. La leyenda “Sin restricción”, al direccionamiento IP que esté en el rango dentro de esa regla tendrán acceso sin limitaciones. Además, en el caso de “Ámbito laboral” y “Ámbito educativo”, el perfil será el mismo; sin embargo, se mantendrán separados los perfiles en caso de que se presente la situación en el que un sitio que sea necesario de revisar, pero esté integrado a las listas negras, se pueda eliminar por perfil.

Antes de la configuración, es necesario que se descargue el compilado de sitios maliciosos que se deben de restringir en el proxy. Hay instituciones que, entre sus actividades se dedican a recopilar los nombres de dominio y URLs no adecuados y estas con conocidas como “Listas Negras” (blacklists), algunas listas son comerciales, otras son de acceso libre. En este trabajo se utilizarán las listas generadas por la Universidad de Toulouse, de Francia. Se descargarán por medio del comando WGET que descarga contenido de la web. Las listas blancas, como sitios de educación y de cultura también vienen incluidas en el directorio que se descargará; sin embargo, son de sitios web franceses, en este caso no es indispensable que las listas blancas se tomen en cuenta.

```
# pkg_add -i wget

wget-1.13.4:libiconv-1.14: ok
wget-1.13.4:gettext-0.18.1p3: ok
wget-1.13.4:libidn-1.25: ok
wget-1.13.4: ok
#
```

Instalado WGET, se crea el directorio /etc/squidguard/db/ en el que se almacenarán las listas negras. También se creará el directorio /etc/squidguard/log/ y se creará el archivo squidGuard.log que registrará el accionar de SquidGuard y de las peticiones web llevadas a cabo. En el directorio etc/squidguard/db/ se descargará el archivo comprimido con las listas, se tiene que descomprimir por medio del comando *tar* y cambiar de dueño, este directorio pertenecerá al usuario y grupo de _squid, creado en la instalación de Squid.

```
# pwd
/etc/squidguard/db
#
# wget ftp://ftp.univ-tlse1.fr/pub/reseau/cache/squidguard_contrib/blacklists.tar.gz
--2013-05-07                              14:52:33--                                ftp://ftp.univ-
tlse1.fr/pub/reseau/cache/squidguard_contrib/blacklists.tar.gz          => `blacklists.tar.gz'
Resolving ftp.univ-tlse1.fr (ftp.univ-tlse1.fr)... 193.49.48.249
Connecting to ftp.univ-tlse1.fr (ftp.univ-tlse1.fr)|193.49.48.249|:21... connected.
Logging in as anonymous ... Logged in!
==> SYST ... done.    ==> PWD ... done.
==> TYPE I ... done.  ==> CWD (1) /pub/reseau/cache/squidguard_contrib ... done.
==> SIZE blacklists.tar.gz ... 7810892
==> PASV ... done.    ==> RETR blacklists.tar.gz ... done.
Length: 7810892 (7.4M) (unauthoritative)

100%[=====================================================>] 7,810,892    109K/s   in 44s

2013-03-07 14:53:23 (172 KB/s) - `blacklists.tar.gz' saved [7810892]

# ls
blacklists.tar.gz
# tar xzf blacklists.tar.gz
# ls
blacklists         blacklists.tar.gz
# cd blacklists
# ls
README             cooking            liste_bu           redirector
ads                dangerous_material mail               remote-control
adult              dating             malware            sect
```

```
aggressive          drogue              manga               sexual_education
agressif            drugs               marketingware       shopping
arjel               filehosting         mixed_adult         social_networks
astrology           financial           mobile-phone        sports
audio-video         forums              phishing            strict_redirector
bank                gambling            porn                strong_redirector
blog                games               press               translation
celebrity           global_usage        proxy               tricheur
chat                hacking             publicite           violence
child               jobsearch           radio               warez
cleaning            lingerie            reaffected          webmail
#
# chown -R _squid:_squid /etc/squidguard/
```

Dentro del directorio que se ha descargado, se tiene una serie de subdirectorios, cada uno con dos o más archivos, los más comunes, "domains", "urls" y uno con el nombre de "usage". El primero de ellos guarda una lista de dominios que almacenan cierto tipo de información o servicio según la categoría que está indicada en el nombre del subdirectorio, por ejemplo, el subdirectorio "chat" contiene varios dominios de sitios web destinados al servicio de mensajería instantánea. Lo mismo ocurre con el archivo "urls" que contiene un conjunto de dominios seguidos de sus URL. El archivo nombrado "usage" tiene información de cómo puede ser utilizada la categoría y lo distingue con un "black" o "white", entre otros valores, el que contiene *black* es una sugerencia de restringir por completo su acceso, los marcados con "White" pueden ser permitidos, o los dos valores, según las políticas de la institución de la cual se trate, puede o no estar permitido.

Ya con las listas de acceso y el software instalado se prosigue a la configuración de las reglas de filtrado. Se despliega el archivo de configuración */etc/squidguard/squidguard.conf* a continuación:

```
logdir /etc/squidguard/log
dbhome /etc/squidguard/db/blacklists

time workhours {
        weekly mtwhf 08:00 - 19:30
}

src admin {
        ip              172.16.9.248-172.16.9.254
}
src directivo {
        ip              172.16.9.247 172.16.9.246
}
src personal {
        ip              172.16.9.235-172.16.9.245
}
src profesores {
        ip              172.16.9.220-172.16.9.234
}
src alumnos {
        ip              172.16.9.1-172.16.9.209
}

dest porn {
       domainlist     porn/domains
       urllist        porn/urls
       expressionlist porn/very_restrictive_expression
       redirect       http://127.0.0.1/bloqueado.php?url=%u
}
dest adult {
       domainlist     adult/domains
       urllist        adult/urls
```

```
        expressionlist adult/very_restrictive_expression
        redirect       http://127.0.0.1/bloqueado.php?url=%u
}

#...(UN DESTINO POR CADA CATEGORÍA DEFINIDA EN EL DIRECTORIO BLACKLIST, SEGÚN EL NIVEL DE
RESTRICCIÓN QUE SE DESEE ESTABLECER )...#

dest violence {
        domainlist     adult/domains
        urllist        adult/urls
        expressionlist adult/expressions
        redirect       http://127.0.0.1/bloqueado.php?url=%u
}

acl {
         admin within workhours {
                 pass !adult !porn all
         } else {
                 pass     any
         }
         directivo within workhours {
                 pass !adult !porn all
         } else {
                 pass     any
         }
         personal {
                 pass !adult !porn !celebrity !gambling all
        }
         profesores {
                 pass !adult !porn !celebrity !gambling all
        }
         alumnos {
                 pass  !adult  !porn  !lingerie  !remote-control  !malware  !manga  !sect  !mixed_adult
!games !warez !strong_redirector !strict_redirector !redirector all
        }
         default {
                 pass none
                 redirect http://127.0.0.1/bloqueado.php?url=%u
         }
}
```

Este archivo de configuración de SquidGuard es el que representa las políticas de navegación en Internet para la red local. Por medio de la directiva *logdir* se establece el directorio donde reside el archivo de registro de SquidGuard, este ya había sido mencionado antes en este trabajo durante la instalación del plug-in. Asimismo, se define la ubicación de los archivos para la creación de la base de datos de Berkeley, esto por medio de la instrucción *dbhome* donde se establece el lugar en el que se encuentra las listas negras que se utilizarán para le filtrado.

A través de la estructura *time workhours* de SquidGuard que define el periodo de lunes a viernes de 8:00 de la mañana a 7:30 de la noche, esto para establecer ciertos periodos en la que se hace filtrado de cierto contenido a determinados usuarios.

Por medio de la estructura *src* se indican las fuentes de peticiones de acceso web, se reconocen con un nombre y se les asigna la dirección o rangos de direccionamiento IP con el que se identificarán. Se establecieron los cinco perfiles exceptuando el de dispositivos de acceso local.

Además, por medio del arreglo *dest* definimos los criterios que se van a revisar en la red, ahí se ejemplifican los destinos porn, adult y violence, pero tienen que ser todos los que se vayan a utilizar para hacer más específico el filtrado. En estas definiciones, se puede especificar que se va a filtrar, en los ejemplos se especifica que se filtren dominios por medio de *domainlist*, URLs con *urllist*, y expresiones regulares con *expressionlist*. Asimismo, en caso

de que una de las entradas al servidor proxy coincida con uno de los criterios con los que se está revisando, a través de la directiva *redirect* se lanza a un sitio web de advertencia en el que se indica al usuario que ha intentado acceder a un sitio no permitido.

El arreglo de acl es el que determina los criterios que se van a filtrar por cada perfil que se definió en la parte superior. Por ejemplo, la fuente de admin, dentro de las horas de trabajo dejará salir cualquier petición web a Internet, excepto alguno que se relaciones con contenido pornográfico y para adultos. Después del periodo de trabajo, el acceso es libre. Esta ACL es la misma para las fuentes que provengan de los directivos de la institución.

Para las peticiones que provengan de direcciones IP del personal administrativo, de confianza y profesores se tratará de la misma manera. Se tendrá acceso a todo, excepto a contenido pornográfico, contenido para adulto, sitios de juegos y sitios de farándula. Esto es todo el tiempo.

El perfil más restringido es el tráfico web que provenga de equipos que usen los alumnos de la institución. Los sitios que se deniegan son los que tiene contenido para adulto, pornografía, violencia, piratería, virus informáticos juegos y manga.

Ya configurado SquidGuard, se pueden crear o actualizar los archivos .db de la base de datos. Esto se hace por medio de la siguiente sentencia, en la que –u especifica que existe una actualización para los archivos .db y –C especifica el archivo del que se crearán las nuevas .db de las urls y dominios que establece el archivo. Este comando puede tardar mucho tiempo hasta que termine de ejecutarse.

```
# squidGuard -u -C /etc/squidguard/squidguard.conf
```

En el archivo de configuración, cualquier petición que coincida con alguno de los criterios de bloqueo será redirigido a una página web que indicará que se está bloqueando un sitio web indebido, este sitio de redirección es proveniente del propio Squid, por lo es necesario habilitar el servidor Web en el equipo Web que es una actividad muy sencilla.

Para activar el servidor web en OpenBSD, es necesario adicionar la línea *httpd_flags="-u"* (el valor –u es utilizado para que el servicio no cree procesos hijos que cambien los valores del directorio de root) en el archivo */etc/rc.conf* y ejecutar el comando *apachectl start* para que se lance el proceso y se abra el puerto 80.

```
# grep "httpd" /etc/rc.conf
# use -u to disable chroot, see httpd(8)
#httpd_flags=NO         # for normal use: "" (or "-DSSL" after reading ssl(8))
httpd_flags="-u"
# apachectl start
/usr/sbin/apachectl start: httpd started
# netstat -an | grep *.80
tcp          0      0  *.80                   *.*                    LISTEN
#
```

Los archivos web para el servidor web, por ejemplo, la página de bloqueo que se mostrará a los usuarios debe de almacenarse en el directorio /var/www/htdocs/.

```
# pwd
/var/www/htdocs
# ls
apache_pb.gif      bsd_small.gif      logo24.jpg         openssl_ics.gif
bgplg              index.html         mod_ssl_sb.gif     smalltitle.gif
bloqueado.html     lock.gif           openbsd_pb.gif
blowfish.jpg       logo23.jpg         openbsdpower.gif
#
```

Después de haberse creado los archivos .db, se procede a modificar el archivo de configuración de Squid para que las peticiones al puerto web que se redirijan al puerto 3128 de Squid sean procesados por SquidGuard. Esa línea se ingresa en el archivo de configuración de Squid */etc/squid/squid.conf*, y se reconfigura el servicio de Squid por medio del comando *squid –k* y su argumento *reconfigure*.

```
redirect_program /usr/local/bin/squidGuard -c /etc/squidguard/squidguard.conf -d
# grep "squidGuard" /etc/squid/squid.conf
redirect_program /usr/local/bin/squidGuard -c /etc/squidguard/squidguard.conf -d
#url_rewrite_program   /usr/local/bin/squidGuard
#
# squid -k reconfigure
#
```

Asimismo, es necesario generar una regla en el Packet Filter de OpenBSD para que el tráfico proveniente de la LAN vaya al puerto 3128 de Squid, y aplicar las reglas por medio del comando *pfctl –f /etc/pf.conf*.

```
EXT="vic0"

INT="vic1"
RED="172.16.0.0/16"
block all
pass in on $INT from $RED
pass in on $INT proto tcp from $RED to any port 80 rdr-to 127.0.0.1 port 3128
match out quick on $EXT from $RED to any nat-to $EXT
<Sólo se muestran las primeras reglas, se remarca la regla que nos interesa>
```

De esta manera ya se tiene configurado y funcionando el filtrado de contenido con las reglas según las políticas que se plantearon al principio. Sin embargo, ¿qué pasa si un dominio o URL de alguno de los grupos de usuarios tiene denegado el acceso a un sitio válido? Se supone a continuación el siguiente ejemplo. El grupo de profesores no puede acceder al dominio mysitioprofesor.com que por alguna razón se encuentra en la lista negra o coincide con alguna expresión regular. Para permitir el acceso se tendría que hacer lo siguiente:

Se crea el subdirectorio /profesores dentro directorio /etc/squidguard/db/blacklists y crear dentro los archivos domains y urls. Cambiar los permisos de los mismos asignándolos al usuario y grupos de _squid.

```
# cd /etc/squidguard/db/blacklists
# pwd
/etc/squidguard/db/blacklists
# mkdir profesores
# cd profesores
# touch domains
# touch urls
# pwd
/etc/squidguard/db/blacklists/profesores
# ls
domains urls
# ls -la
total 8
drwxr-xr-x   2 root    _squid   512 Mar  7 19:15 .
drwxr-xr-x  50 _squid  _squid  1536 Mar  7 19:15 ..
-rw-r--r--   1 root    _squid     0 Mar  7 19:15 domains
-rw-r--r--   1 root    _squid     0 Mar  7 19:15 urls
# chown -R _squid:_squid /etc/squidguard/db/blacklists/pro
profesores/  proxy/
# chown -R _squid:_squid /etc/squidguard/db/blacklists/profesores/
# ls -ls
total 0
```

```
-rw-r--r--  1 _squid  _squid  0 Mar  7 19:15 domains
-rw-r--r--  1 _squid  _squid  0 Mar  7 19:15 urls
#
```

Dentro del archivo creado llamado domains, se agrega el sitio al que se desea permitir acceso al grupo de profesores.

Modificar el archivo de configuración /etc/squidguard/squidguard.conf agregando un destino y modificar la ACL para profesores de la siguiente forma:

```
dest profesores {
        domainlist     profesores/domains
        urllist        profesores/urls
}
acl {
        }
         profesores {
                 pass profesores !adult !porn !celebrity !gambling all
        }
```

En las líneas anteriores, el criterio "profesores" que se ha creado se ubicó en la ACL sin el símbolo de exclamación cerrado "!", la sintaxis de SquidGuard determina que especificar el destino sin el símbolo determina que lo que coincida con él será permitido.

Después de realizarse las modificaciones al archivo de configuración de SquidGuard, se deben actualizar los archivos .db para que tengan efecto los cambios, esto a través del comando squidGuard –u –C */etc/squidguard/squidguard.conf*.

3.4 La seguridad en los dispositivos durante el proceso de mejora continua

Como ya se mencionó anteriormente, la infraestructura de red del IEMS cuenta con Routers bajo el sistema operativo pfSense funcionando. Sin embargo, debe contemplarse una mejora en la estructura de la red pensando en un reemplazo de los dispositivos pfSense por Routers de una marca en específico, por ejemplo, una infraestructura bajo dispositivos de la marca *Cisco*®. De esta manera, el uso de firewalls sobre OpenBSD se puede dejar de hacer, ya que los Routers ofrecen características como el filtrado de paquetes, NAT, entre otras características.

A continuación se muestra la configuración de Listas de Control de Acceso (ACL) que permitirán controlar la gestión de los dispositivos por medio de SSH o Telnet, así como permitir sólo el uso de los servicios de http y https a los usuarios de las redes locales.

3.4.1 Implementación de Listas de control de acceso (ACL)

Es importante mantener el acceso a los recursos y a la administración de los dispositivos controlado. Las redes locales en cada plantel sólo permitirán a sus usuarios acceso a los servicios web http y http seguro (https). Sin embargo, hay un grupo de direcciones IP en cada uno de los planteles que tendrá acceso a todos los servicios externos a la administración de los Routers, siendo esta última de gran importancia para la determinación y solución de problemas que se presenten en la red.

Una de las características que ofrecen los dispositivos de red Cisco® es la implementación de Listas de Control de Acceso que son configuradas en cada uno de los dispositivos siguiendo determinadas reglas para restringir o permitir el acceso de una red a otra por medio de una lista de sentencias.

3.4.2 Control de acceso a las líneas de terminal

Se requieren Listas de control de acceso en todos los Routers de los planteles para permitir la administración del dispositivo sólo a equipos pertenecientes a los administradores. En cada plantel habrá 7 equipos administradores con los permisos para acceder a los Routers para administración remota.

La dirección IP que iniciará el segmento de equipos administradores será la 248, por ejemplo, en la red del plantel 1 Lázaro Cárdenas que cuenta con la red local 172.16.1.0/24, el rango de direcciones perteneciente a los administradores será la 172.16.1.248 hasta la dirección 172.16.1.255. El rango de direcciones puede ser representado por medio de una máscara de Wildcard a la máscara de subred 255.255.255.248 que se utilizará en la sentencia de las ACL. Las máscaras de Wildcard son importantes durante la configuración de ACL debido a que al igual que una máscara de subred en la configuración de algún dispositivo, una máscara de Wildcard especifica un rango de direcciones que se tomarán en cuenta para cierto criterio específico, en este caso, la denegación o permisión de algún servicio.

En el plantel Lázaro Cárdenas tiene las siguientes direcciones IP para los equipos que pertenecen a los administradores de red: 172.16.1.248, 172.16.1.249, 172.16.1.250, 172.16.1.251, 172.16.1.252, 172.16.1.253, 172.16.1.254 y 172.16.1.255.

De las direcciones anteriores, sólo se podrán utilizar siete de ellas, la dirección 172.16.1.255 no se podrá utilizar ya que representa la dirección de broadcast de la red y no puede ser asignada a ningún dispositivo.

Para comprobar que cada dirección IP del rango que se ha establecido para los equipos de los administradores es válida para la máscara de Wildcard que se utilizará, se convertirán la dirección IP a comprobar y la máscara de Wildcard a su equivalente binario. Realizado lo anterior, se compararán bit a bit por posición, En las Listas de control de acceso, la máscara de Wildcard tiene la función de ignorar los bits de la dirección IP que coincidan con los bits encendidos de la máscara de Wildcard considerándolos como ceros.

La dirección 172.16.1.248 con máscara de Wildcard 0.0.0.7 es la dirección que se tomará en cuenta durante las comprobaciones, ya que es el identificador de red del rango de las direcciones que se han establecido.

Para realizar la comprobación que haría el Router al comparar una dirección IP con alguna ACL especificada con cierta dirección con máscara de Wildcard. Se tomará de ejemplo la llegada de un paquete proveniente de un mensaje de correo electrónico, este tiene en su cabecera una dirección IP del equipo fuente, la dirección la dirección IP 172.16.1.232, que será comprobada por el dispositivo utilizando la máscara de Wildcard resultando lo siguiente:

Dirección: 172.16.1.232	00001010.00011110.00000001.11101000
Máscara Wildcard: 0.0.0.7	00000000.00000000.00000000.00000111
Resultado: 172.16.1.232	00001010.00011110.00000001.11101000

Para que la dirección IP sea válida, después de la comparación con la máscara de Wildcard, el resultado debe de ser 172.16.1.248, el identificador del rango de direcciones tomadas para los administradores la red 172.16.1.0/24. La dirección 172.16.1.232 es diferente a la dirección 172.16.1.248, no es válida para la sentencia de Wildcard. Ahora se verifica con una dirección IP que si es válida para la sentencia con Wildcard:

Dirección: 172.16.1.250	00001010.00011110.00000001.11111010
Máscara Wildcard: 0.0.0.7	00000000.00000000.00000000.00000111
Resultado: 172.16.1.248	00001010.00011110.00000001.11111000

La dirección que resultó es igual a 172.16.1.248, por lo que es válida para la sentencia de Wildcard. Este procedimiento es el que sigue el Router cuando recibe un paquete con cierta dirección IP en la cabecera, verifica cada una de las sentencias de la ACL, si alguna coincide por medio de este método, se aplica la regla correspondiente.

Las ACL en cada Router deben de tomar en cuenta los siguientes grupos de direcciones IP. Estás direcciones se han originado de cada una de las redes locales que se calcularon en el capítulo dos de este trabajo:

172.16.1.248/29	172.16.2.248/29	172.16.3.248/29	172.16.4.248/29
172.16.5.248/29	172.16.6.248/29	172.16.7.248/29	172.16.8.248/29
172.16.9.248/29	172.16.10.248/29	172.16.11.248/29	172.16.12.248/29
172.16.13.248/29	172.16.14.248/29	172.16.15.248/29	172.16.16.248/29
172.16.17.248/29	172.16.18.248/29	172.16.19.248/29	172.16.20.248/29

Además, si un administrador logra el acceso a algún Router, a través de este se podría acceder a otro Router. Por esta razón, también se debe establecer una ACL o conjunto de ACL que determine que los Routers pueden ser accesibles entre sí el uno del otro.

Las direcciones de las interfaces de los Routers van de la dirección 172.16.30.2 a la 172.16.30.78 que se establecieron en el capítulo dos durante el cálculo del direccionamiento. Debido a esa información, se pueden establecer dos direcciones con su respectiva máscara de Wildcard que englobe todas las direcciones dentro de ese rango.

- 172.16.30.0 0.0.0.63
- 172.16.30.64 0.0.0.15

La primera de ellas comprende a las direcciones entre la dirección 172.16.30.0 a la dirección 172.16.30.63, mientras que la segunda comprende de la dirección 172.16.30.64 a la dirección 172.16.30.79.

Se puede comprobar alguna dirección que no está en el rango, por ejemplo, 172.16.30.82.

Dirección: 172.16.30.82	00001010.00011110.00011110.01010010
Máscara Wildcard: 0.0.0.15	00000000.00000000.00000000.00001111
Resultado: 172.16.30.80	00001010.00011110.00011110.01010000

La dirección 172.16.30.80 no es igual a 172.16.30.64 o 172.16.30.0.

La dirección 172.16.30.78	00001010.00011110.00011110.01001110
Máscara Wildcard: 0.0.0.15	00000000.00000000.00000000.00001111
Resultado: 172.16.30.64	00001010.00011110.00011110.01000000

La dirección que resultó es la misma que la que determina el rango de direcciones.

Todos los Routers tendrán la misma ACL que permite que los equipos administradores de cada plantel tengan acceso a los dispositivos remotamente. Esto es independiente del protocolo implementado, SSH o telnet.

```
ip access-list standard 10
 permit 172.16.1.248 0.0.0.7
 permit 172.16.2.248 0.0.0.7
 permit 172.16.3.248 0.0.0.7
 permit 172.16.4.248 0.0.0.7
 permit 172.16.5.248 0.0.0.7
 permit 172.16.6.248 0.0.0.7
 permit 172.16.7.248 0.0.0.7
 permit 172.16.8.248 0.0.0.7
 permit 172.16.9.248 0.0.0.7
 permit 172.16.10.248 0.0.0.7
 permit 172.16.11.248 0.0.0.7
 permit 172.16.12.248 0.0.0.7
 permit 172.16.13.248 0.0.0.7
 permit 172.16.14.248 0.0.0.7
 permit 172.16.15.248 0.0.0.7
 permit 172.16.16.248 0.0.0.7
 permit 172.16.17.248 0.0.0.7
 permit 172.16.18.248 0.0.0.7
 permit 172.16.19.248 0.0.0.7
 permit 172.16.20.248 0.0.0.7
 permit 172.16.30.0 0.0.0.63
 permit 172.16.30.64 0.0.0.15      ¡Administración Router a Router
 permit 10.0.1.248 0.0.0.7
 permit 10.0.2.248 0.0.0.7         ! Administración desde las oficinas centrales.
 permit 10.0.3.248 0.0.0.7
```

La ACL es estándar numerada con el valor de 10, no se especifican puertos ni destinos, sólo es necesario especificar el origen de las peticiones.

La ACL se aplica a las líneas de *VTY*[13] de la siguiente manera:

```
line vty 0 4
 access-class 10 in
!
```

Esta ACL es configurada en todos los Routers, todos tiene la misma administración común ya que pertenecen a un sistema autónomo local perteneciente al IEMS.

[13] Virtual Terminal Line (Línea de Terminal Virtual) utilizada por diversos dispositivos para acceso remoto a través de Telnet y SSH (Secure Shell).

A través de esta ACL colocada en la configuración de las líneas de terminal remota, sólo los equipos con las direcciones especificadas tendrán acceso a la administración del dispositivo. Asimismo, es posible que desde los propios Routers se pueda acceder a otro Router de manera remota para su administración.

Para que un Router sea administrable remotamente tiene que tener configurados usuarios con ciertos privilegios, contraseña para acceso a modo privilegiado y la correcta configuración de las líneas VTY con el protocolo SSH o Telnet. A estas terminales VTY se les aplica la ACL para poder delimitar los dispositivos que tendrán acceso a él.

Para probar su funcionamiento, se intenta el acceso a al Router del plantel José Revueltas desde un equipo del plantel Lázaro Cárdenas. Se verifica la dirección IP, la conectividad con el Router (un ping a la dirección IP de su interfaz conectada al Router enlace) y el intento de acceso a través de telnet.

```
PC>ipconfig

IP Address......................: 172.16.1.1
Subnet Mask.....................: 255.255.255.0
Default Gateway.................: 172.16.1.254

PC>ping 172.16.30.73

Pinging 172.16.30.73 with 32 bytes of data:

Reply from 172.16.30.73: bytes=32 time=62ms TTL=254
Reply from 172.16.30.73: bytes=32 time=72ms TTL=254
Reply from 172.16.30.73: bytes=32 time=78ms TTL=254
Reply from 172.16.30.73: bytes=32 time=65ms TTL=254

Ping statistics for 172.16.30.73:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 62ms, Maximum = 78ms, Average = 69ms

PC>telnet 172.16.30.73
Trying 172.16.30.73 ...
% Connection refused by remote host
PC>
```

El resultado de intento de conexión arrojó el mensaje "*Connection refused by remote host*" que indica que se ha negado el intento de conexión al dispositivo.

Ahora se prueba la ACL con el equipo administrador del plantel Lázaro Cárdenas para acceder a la administración del Router José Revueltas:

```
PC>ipconfig

IP Address......................: 172.16.2.111
Subnet Mask.....................: 255.255.255.0
Default Gateway.................: 172.16.2.254

PC>ping 172.16.30.73

Pinging 172.16.30.73 with 32 bytes of data:

Reply from 172.16.30.73: bytes=32 time=65ms TTL=254
Reply from 172.16.30.73: bytes=32 time=46ms TTL=254
Reply from 172.16.30.73: bytes=32 time=92ms TTL=254
Reply from 172.16.30.73: bytes=32 time=65ms TTL=254

Ping statistics for 172.16.30.73:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
    Minimum = 46ms, Maximum = 92ms, Average = 67ms

PC>telnet 172.16.30.73
Trying 172.16.30.73 ...Open


User Access Verification

Username:
```

Se puede observar que el intento de conexión de este equipo al Router fue aceptada, esto se debe a que la sentencia de ACL permitió al dispositivo con IP 172.16.1.111 con el Router.

3.4.3 Implementación de ACL de control de salida a Internet

Se tiene que restringir el acceso a los recursos externos desde las redes locales, los usuarios en cada plantel sólo tendrán acceso WEB a través del puerto 80 y el puerto 443 (WEB seguro). Los equipos administradores tendrán acceso a cualquier servicio en redes externas.

El envío de mensajes a través del protocolo ICMP (Internet Control Messages Protocol) implementado por el comando PING utilizado para probar conectividad con otras redes será permitido a todos los equipos dentro de la red del IEMS. Sin embargo, los mensajes PING del exterior al interior serán negados. Otro servicio que será permitido será el de las peticiones UDP a los servidores de DNS a través del puerto 53, se aprobará a todos los equipos de la red de la Institución.

Todas las redes de los planteles se pueden agrupar en una dirección IP con determinada máscara de subred que sumarice.

Las redes se pueden sumarizar va del rango de 172.16.1.0/24 a la red 172.16.20.0/24:

172.16.1.0
172.16.00000001.00000000
172.16.00010100.00000000
172.16.20.0
Sumarización: 172.16.0.0/19

La red 172.16.0.0/19 incluye a las redes 172.16.1.0 a la 172.16.1.20 y más, ya que la máscara también incluye redes como la 172.16.24.0 debido a que el rango resultado de la sumarización la incluye.

Asimismo, los conjuntos de IP administradoras que se habían establecido para el acceso a los Routers también serán tomados en cuenta para escribir la sentencia que permite el tráfico de estás a cualquier servicio. Por ejemplo, en el plantel 1 Lázaro Cárdenas el conjunto de direcciones IP 172.16.1.248 a la 172.16.1.254 tienen permitido el acceso total a recursos externos. Estás direcciones se pueden representar de la siguiente manera:

172.16.1.248/29 que se debe de tomar en cuenta antes que las sentencias que incluye a todas las redes debido a que las ACL se analizan de la regla más específica a la general.

Las sentencias que delimitan a las redes locales son:

```
ip access-list extended SERVICIOS_PERMITIDOS
 permit ip 172.16.1.248 0.0.0.7 any
 permit ip 172.16.2.248 0.0.0.7 any
 permit ip 172.16.3.248 0.0.0.7 any
```

```
 permit ip 172.16.4.248 0.0.0.7 any
 permit ip 172.16.5.248 0.0.0.7 any
 permit ip 172.16.6.248 0.0.0.7 any
 permit ip 172.16.7.248 0.0.0.7 any
 permit ip 172.16.8.248 0.0.0.7 any
 permit ip 172.16.9.248 0.0.0.7 any
 permit ip 172.16.10.248 0.0.0.7 any
 permit ip 172.16.11.248 0.0.0.7 any
 permit ip 172.16.12.248 0.0.0.7 any
 permit ip 172.16.13.248 0.0.0.7 any
 permit ip 172.16.14.248 0.0.0.7 any
 permit ip 172.16.15.248 0.0.0.7 any
 permit ip 172.16.16.248 0.0.0.7 any
 permit ip 172.16.17.248 0.0.0.7 any
 permit ip 172.16.18.248 0.0.0.7 any
 permit ip 172.16.19.248 0.0.0.7 any
 permit ip 172.16.20.248 0.0.0.7 any
 permit tcp 172.16.0.0 0.0.255.255 any eq www
 permit tcp 172.16.0.0 0.0.255.255 any eq 443
 permit udp any any eq 53
 permit icmp any any echo
!
```

Estas sentencias se aplican a la interfaz de salida del Router que enlaza a todos los planteles, tal como se puede observar en la figura 3.20.

```
interface FastEthernet0/1
 ip access-group SERVICIOS_PERMITIDOS out
!
```

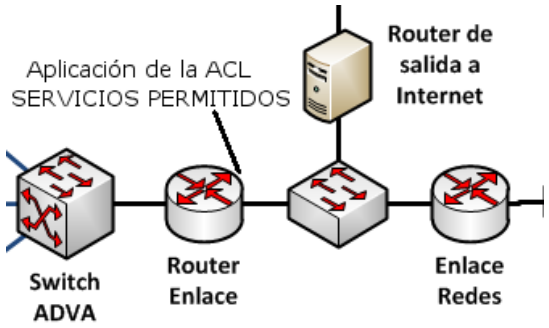

Figura 3.69. Ubicación de la ACL *SERVICIOS PERMITIDOS* en la red.

La ACL se asoció a la interfaz como OUT debido a que se analizará el tráfico que saldrá de esta. De esta manera, cada paquete que vaya a salir del dispositivo será analizado para verificar si es denegada o permitida por el dispositivo según la regla con la que el paquete saliente concuerde.

De esta manera, los equipos en una LAN de cualquier plantel sólo tendrán acceso al servicio WEB por medio de HTTP o HTTPS (WEB seguro). Cualquier otro servicio será denegado, por ejemplo, FTP (File Transfer Protocol). A continuación se verifica la ACL en un equipo local del plantel Lázaro Cárdenas:

```
PC>ipconfig

IP Address......................: 172.16.1.1
Subnet Mask.....................: 255.255.255.0
Default Gateway.................: 172.16.1.254

PC>ping 209.168.201.8

Pinging 209.168.201.8 with 32 bytes of data:

Reply from 209.168.201.8: bytes=32 time=111ms TTL=125
Reply from 209.168.201.8: bytes=32 time=141ms TTL=125
Reply from 209.168.201.8: bytes=32 time=202ms TTL=125
Reply from 209.168.201.8: bytes=32 time=129ms TTL=125

Ping statistics for 209.168.201.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 111ms, Maximum = 202ms, Average = 145ms

PC>ftp 209.168.201.8
Trying to connect...209.168.201.8

%Error opening ftp://209.168.201.8/ (Timed out)
```

El comando PING fue aceptado como se determinó, no así el intento de acceso a un servidor FTP exterior, la conexión no se logró efectuar.

Ahora se comprueba el acceso por medio de un equipo administrador:

```
PC>ipconfig

IP Address......................: 172.16.1.250
Subnet Mask.....................: 255.255.255.0
Default Gateway.................: 172.16.1.254

PC>ping 209.168.201.8

Pinging 209.168.201.8 with 32 bytes of data:

Reply from 209.168.201.8: bytes=32 time=156ms TTL=125
Reply from 209.168.201.8: bytes=32 time=125ms TTL=125
Reply from 209.168.201.8: bytes=32 time=141ms TTL=125
Reply from 209.168.201.8: bytes=32 time=124ms TTL=125

Ping statistics for 209.168.201.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 124ms, Maximum = 156ms, Average = 136ms

PC>ftp 209.168.201.8
Trying to connect...209.168.201.8
Connected to 209.168.201.8
220- Welcome to PT Ftp server
Username:
```

Se puede observar esta vez que este equipo si puede realizar una conexión a un servidor FTP externo ya que la conexión fue abierta y se solicitan datos del servidor para tener un acceso completo.

La asignación de direccionamiento depende de los administradores de red, el que se ha presentado en este documento es una propuesta, pero no es un estándar de industria que se tenga que hacer forzosamente esto.

3.4.4 Controlando sesiones de EIGRP usando la autenticación

Una de las características que ofrece el protocolo EIGRP y la mayoría de los protocolos de ruteo es la integración de la autenticación de sus mensajes. De manera predeterminada, los mensajes transmitidos por los enrutadores por medio de EIGRP lo hacen sin autenticar.

Es importante que todos los equipos en el dominio de ruteo de la institución educativa implementen un mecanismo para que se verifique la autenticidad de los Routers, de los mensajes de ruteo compartido y a su vez de la integridad de los datos que se comparten.

Actualmente existen muchos sistemas operativos que son capaces de implementar un protocolo de ruteo y compartir información, muchos de estos se basan en Linux. Si un equipo no autorizado se integra a la red, este configurado en él un protocolo de ruteo dinámico, por ejemplo, EIGRP. Esto puede causar comportamientos no deseados que afecten al servicio gravemente. Entre los problemas que podrían originarse se mencionan algunos a continuación:

- Al establecerse una sesión de EIGRP con el equipo intruso que también conoce EIGRP, este conocerá las redes que se tienen anunciadas debido a que los Routers comparten con él su información de ruteo.
- Se puede enviar información falsa de rutas ya existentes pero con la manipulación de las métricas haciéndolas más bajas para que sean preferidas por los enrutadores de la red. Al ocurrir un escenario así, las tablas de ruteo van a instalar las mejores rutas debido a la métrica menor y enviar paquetes destinados a esas rutas hacia el nuevo camino anunciado. En equipo intruso recibe la información que ha sido enrutada por todos los Routers hacia él y la analiza a través de un analizador de protocolos con un fin determinado. De esta manera se ha denegado el servicio de los usuarios que salían a algún servicio a través de esas rutas ya que se ha influenciado el tráfico de la red por caminos y se ataca a la confidencialidad.
- Debido a que se ha integrado un intruso que los equipos de la red conocen como vecino y envían información, este a su vez genera tráfico falso a todas las redes o alguna en específica y le genera una denegación de servicio.

A pesar de que EIGRP es un protocolo propietario de Cisco®, la situación no ha impedido que haya variantes desarrolladas en diversos sistemas operativos libres, por ejemplo en Linux. En concreto, *Quagga* es un conjunto de software para configurar protocolos de ruteo y puede ejecutarse en las principales distribuciones de Linux. Sin embargo, debido a que EIGRP es de uso propietario, no se ha desarrollado alguna variante de él para que se ejecute en ese sistema, los protocolos que soporta son OSPF, IS-IS, RIPv2 y BGP y es una ventaja, pero no es suficiente. Hay algunos desarrollos sobre Java[14] que logran enviar mensajes de EIGRP, estos fueron creados para su uso didáctico, pero pueden ser utilizados de manera diferente en las manos equivocadas.

También existe GNS3, un poderoso simulador de redes gráfico con la capacidad de configurar varias características de diferentes sistemas operativos de red, entre ellos el sistema operativo de Cisco®, IOS. Este proyecto de Fuente abierta (Open Source) puede ser instalado y ejecutado en cualquier sistema operativo, incluyendo Windows y Linux. Entre sus características, puede conectarse el equipo que ejecuta GNS3 y su red

[14] Java es un lenguaje de programación orientado a objetos, basado en clases, concurrente y de propósito general. Su objetivo es permitir a los desarrolladores de software "escribir una vez, ejecutar en cualquier parte", que significa que un programa que se ejecuta en una computadora no necesita recompilarse para ejecutarse en otra.

simulada a una red local física a través de las interfaces del equipo. Sin los mecanismos de seguridad aplicados en nuestra red, esto podría causarnos problemas serios, pues a través del equipo que tiene la red simulada se pueden crear diversos paquetes con información, entre ellos de ruteo, desviar el tráfico hacia sí mismo y por medio de un analizador de protocolos, examinarlo, pero a su vez provocando también una denegación de servicio debido a que el tráfico no está llegando a su destino.

En el capítulo anterior, durante la configuración de EIGRP en los Routers, se mencionó el comando *passive-interface default*. Este comando configurado en el proceso de EIGRP indica al protocolo de ruteo que ninguna interfaz del equipo intervendrá en el proceso de ruteo para el envío y recepción de información de ruteo por y hacia los equipos que estén conectados adyacentes a las interfaces, es decir, son pasivas a EIGRP. De esta manera, sólo las interfaces a las que se desea que compartan información de ruteo se utiliza el *no passive-interface [interfaz <slot>]* para que dejen de ser pasivas en el proceso de ruteo, creen adyacencias con sus vecinos y compartan información de ruteo.

Ahora, para entender lo que se tratará en los siguientes párrafos, hay que entender cómo trabajan las funciones hash, en especial MD5.

Para mantener un documento digital que se va a transmitir a través de una red, para mantenerlo el usar un algoritmo criptográfico simétrico sería computacionalmente alto en lo que respecta al procesamiento de las operaciones, tanto en el emisor que cifra y el receptor que descifra, por tal razón las funciones hash son una herramienta demasiado útil en la transmisión de información a través de internet. Una función hash sirve como una firma digital de un documento o mensaje. A partir de un documento digital, la función hash genera un resumen comprimido sin importar el tamaño en disco del documento que se desea firmar, el resultado es un bloque ilegible de longitud fija que representa toda la información que se le ha dado como entrada. Estas funciones no tienen el mismo propósito de la criptografía simétrica y asimétrica, ya que, generado el resumen del documento, no se tiene un regreso de la entrada original, es un proceso irreversible.

Las principales aportaciones que hacen las funciones hash son las siguientes:

- *Proporcionan autenticidad*: Cuando el receptor recibe le mensaje junto con la firma que se generó a partir de la función hash, este toma el mensaje y a través de su clave local y su función hash genera un resumen del documento, si al comparar el resumen con el que venía en el mensaje, es auténtico, ya que se puede corroborar que el emisor tiene la misma clave que se pactó desde un acuerdo posterior.
- *Comprueban la integridad de la información*: Si la información que se envió fue modificada durante la transmisión/recepción, al realizar el resumen del mismo, este no coincidirá con el que viene acompañado del mensaje.

En lo que concierne al algoritmo de MD5, fue desarrollado por Ron Rivest del Instituto tecnológico de Massachusetts en 1992 como un algoritmo más robusto a su antecesor MD4 (dado a conocer en 1990). Actualmente es uno de los algoritmos más ampliamente usados por su robustez, como en la autenticación de sitios web por medio del protocolo SSL[15] (Secure Sockets Layers), y en la autenticación de mensajes en diferentes protocolos de ruteo, entre ellos OSPF, EIGRP, BGP y RIP.

Por otra parte, al habilitar la autenticación en EIGRP, causa que los Routers autentiquen cada mensaje. Para que funcione, cada uno de los Routers debe usar la misma clave pre compartida (PSK por sus siglas en inglés, Pre Shared key), generando un resumen MD5 por cada mensaje EIGRP basado en esa PSK. Si un Router configurado con autenticación EIGRP recibe un mensaje de EIGRP y el resumen de MD5 del mensaje no el chequeo de autenticación basado en la copia local de la clave, el Router silenciosamente descarta el mensaje. Como resultado,

[15] Secure Sockets Layer (SSL, en español Capa de Conexión Segura) y su sucesor Transport Layer Security (TLS, en español Seguridad de la Capa de Transporte) son protocolos criptográficos que proporcionan comunicaciones seguras a través de la red.

cuando la autenticación falla, dos Routers no pueden convertirse en vecinos de EIGRP porque ignoran los mensajes *Hello*.

Desde una perspectiva de diseño, la autenticación de EIGRP ayuda a prevenir ataques de denegación de servicio (DoS, Denial of Service por sus siglas en inglés), pero no provee privacidad alguna. Los mensajes de EIGRP pueden ser leídos por cualquier dispositivo que físicamente reciba los bits. Hay que notar en una red LAN, el flujo de actualizaciones son a la dirección IP de multicast 224.0.0.10, por lo que cualquier atacante podría unirse al grupo 224.0.0.10 de multicast y leer los paquetes. Sin embargo, la autenticación previene que los atacantes formen adyacencias con Routers legítimos, previniendo el anuncio de información incorrecta de ruteo.

3.4.4.1 Lista de verificación de la configuración de la autenticación de EIGRP

El proceso de configuración de la autenticación de EIGRP requiere de varios comandos, que son resumidos a continuación:

- Paso1: Creación de una cadena clave de autenticación (key chain):
    - Crear la cadena y darle un nombre con el comando global **key chain** *nombre*. El nombre de la cadena no tiene que coincidir con el de los Routers vecinos.
    - Crear uno o más número de clave usando el comando **key** *número* en el modo de configuración de cadena. El número de clave tiene debe de coincidir con el de los Routers vecinos.
    - Definir el valor de la clave de autenticación con el comando **key-string** *valor* en el modo de configuración de clave. La cadena de la clave debe de coincidir con los Routers vecinos. De manera opcional se pueden definir el valor *lifetime* (periodo de tiempo) para el envío y aceptación de cada cadena de clave.

- Paso 2: Habilitar la autenticación de EIGRP con MD5 en una interface, para un número de sistema autónomo en particular (identificador del proceso de EIGRP), usando el subcomando de interfaz **ip authentication mode eigrp** *[identificador-proceso-eigrp]* **md5**.

- Paso 3: Referirse a la clave correcta a ser usada en la interfaz usando el subcomando de interfaz **ip authentication key-chain** *[identificador-proceso-eigrp] [nombre-de-cadena]*.

Es importante seguir el paso 1 detalle a detalle, los pasos 2 y 3 son relativamente fáciles. Esencialmente, el sistema operativo IOS de Cisco® configura los valores de la clave separadamente (paso 1) y luego requiere un subcomando de interfaz para referirse a los valores de la clave.

Entonces se presenta la configuración que se debe de realizar en los equipos de red del IEMS. Ya se indicó en el capítulo anterior la configuración de las interfaces pasivas en EIGRP. Sin embargo, la configuración de la clave es la siguiente:

```
key chain AUTENTICACION_EIGRP
 key 100
  key-string CLAVE_EIGRP
```

En este caso, el nombre de la cadena de la clave se llamará AUTENTICACION_EIGRP, este puede ser diferente para todos los Routers, pero por convención, se utilizará el mismo. El número de la clave si debe de ser el mismo en todos. Además, dentro del modo de configuración del número de la clave, se encuentra la clave que se utilizará para la realización de los mensajes resumidos por MD5. Esta clave es CLAVE_EIGRP y debe de ser el mismo en todos los Routers con los que se quiera establecer adyacencia. En este documento se eligió esta clave, pero puede ser otra elegida por el administrador definida como una contraseña con caracteres especiales, números y caracteres alfanuméricos.

Asimismo, en el Router principal y en los Routers de los planteles se configurará la misma *key chain* para autenticar los mensajes.

Después de definir la clave, se configuran las interfaces que participarán en el proceso de EIGRP y autenticarán la información. La siguiente configuración mostrada es la que se aplica a una de las subinterfaces en el Router principal:

```
Router(config)#interface FastEthernet0/0.50
Router (config-if)# ip authentication mode eigrp 100 md5
Router (config-if)#ip authentication key-chain eigrp 100 AUTENTICACION_EIGRP
```

Si ya se encontraba establecida la sesión de EIGRP con el Router en el plantel adyacente, esta se perderá, si se enciende el comando de depuración en el Router del extremo en el que aún no se ha establecido la configuración de autenticación, se puede ver lo siguiente:

```
Plantel-5#debug eigrp packets
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY,
SIAREPLY)
EIGRP Packet debugging is on
Plantel-5#
<Información omitida>
*Apr 29 03:54:59.030: EIGRP: FastEthernet0/0: ignored packet from 10.30.30.34, opcode
= 5 (authentication off)
<Información omitida>
```

El paquete de Hello de EIGRP que se ha enviado del Router principal ha sido ignorado, pues este usa autenticación, el Router del plantel no lo tiene activado, se activa a continuación:

```
Plantel-5(config)#key chain AUTENTICACION_EIGRP
Plantel-5(config-keychain)#key 100
Plantel-5(config-keychain-key)#key-string CLAVE_EIGRP
Plantel-5(config-keychain-key)#interface FastEthernet 0/0
Plantel-5(config-if)#ip authentication mode eigrp 100 md5
Plantel-5(config-if)#$cation key-chain eigrp 100 AUTENTICACION_EIGRP
Plantel-5(config-if)#
*Apr 29 04:00:46.126: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 192.168.1.1
(Ethernet0/0) is up: new adjacency
Plantel-5(config-if)#
```

Inmediatamente que se ha establecido la autenticación de los mensajes de EIGRP en la interfaz, la adyacencia levanta. Ahora por medio del comando *debug* se observa cómo se intercambian los mensajes de Hello con autenticación:

```
Plantel-5#debug eigrp packets
    (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY,
SIAREPLY)
EIGRP Packet debugging is on
Plantel-5#
*Apr 29 04:04:17.350: EIGRP: Sending HELLO on FastEthernet0/0 - paklen 60
*Apr 29 04:04:17.350:   AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely
0/0
<Se omite información>
Plantel-5#
```

```
*Apr 29 04:04:18.634: EIGRP: received packet with MD5 authentication, key id = 100
*Apr 29 04:04:18.634: EIGRP: Received HELLO on FastEthernet0/0 - paklen 60 nbr
10.30.30.33
*Apr 29 04:04:18.634:    AS 100, Flags 0x0:(NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely
0/0 peerQ un/rely 0/0
<Se omite información>
```

Se puede observar el envío y la recepción de mensajes de *Hello*. El mensaje enviado no indica que se envía con un mensaje resumido, pero está implícito. Este se envía al sistema autónomo 100, como se conoce en EIGRP, en realidad se trata del dominio de ruteo 100 para EIGRP.

Del mismo modo, se puede ver un mensaje de *Hello* que se ha recibido, este tiene autenticación MD5 y usa una llave con número 100. Si este valor no coincidiera, no se utilizará la clave que se configuró y se descartaría el mensaje.

Para verificar la autenticidad del mensaje, el Router del plantel toma el mensaje que ha recibido y le quita el mensaje resumido de MD5, ingresa el mensaje y su clave local al proceso de resumen de MD5 y compara el resultado con el mensaje, si este coincide, el mensaje viene del Router que se esperaba (el Router principal), y además, se puede comprobar que este no fue modificado durante la transmisión, figura 3.21.

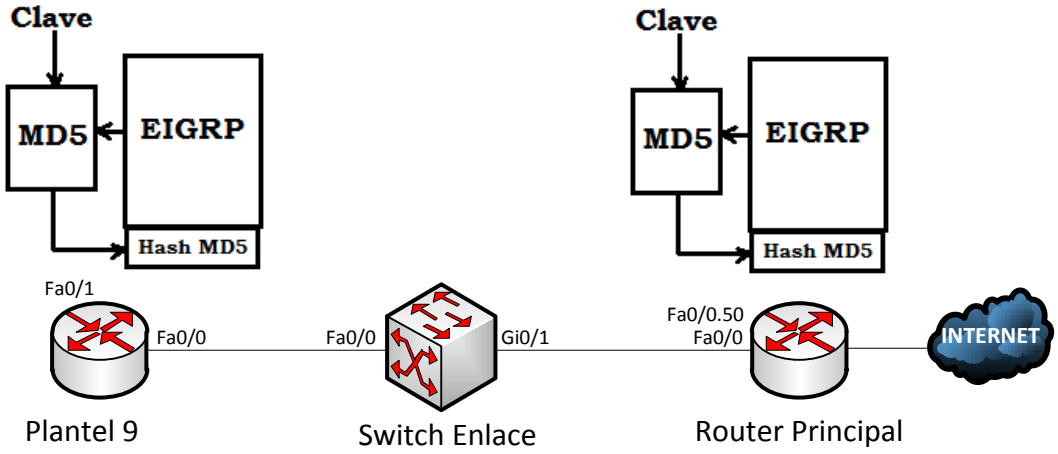

Figura 3.70 Autenticación de mensajes EIGRP

Ahora bien, la configuración que se mostró es plana, es decir, se muestra tal como se ha ingresado al equipo por lo que es conveniente habilitar el servicio de cifrado del equipo. Es un algoritmo débil, pero ya no quedan legibles las contraseñas en la configuración del equipo.

```
service password-encryption
key chain AUTENTICACION_EIGRP
 key 100
  key-string 7 062523007A6B363C2C30203B
```

Ahora la cadena en la línea de comando key-string aparece ilegible, fue cifrada a través de algoritmo de cifrado 7 de cisco. Sin embargo, hay muchos programas que descifran cadenas cifradas por el algoritmo 7, pero se utiliza como alternativa en caso de que hayan ingresado al equipo de manera no autorizada.

3.5 Configuración de la seguridad en el Switch

Los switches de la red local, además de los Routers que reenvían el tráfico entre los planteles y hacia Internet durante la mejora continua necesitan mecanismos de autenticación de usuarios que les permita sólo a una persona o grupo de ellas el gestionarlo ingresando al dispositivo por medio de Telnet o SSH utilizando un nombre de usuario y una contraseña que haya sido previamente configurada en el dispositivo o por medio de un servidor de autenticación como TACACS.

Asimismo, tal como se realizó en el capítulo dos en el que se estableció la configuración de DHCP del Router para la asignación de determinadas direcciones IP a ciertos equipos a través de su dirección MAC, en la conexión física de los equipos se puede especificar un grupo de direcciones MAC permitidas a cierto puertos del Switch de acceso.

Además de relacionar una dirección IP con una dirección MAC para la asignación de direccionamiento a través del servicio de DHCP, se establecerá la seguridad en los puertos de los switches en los que se conectarán cada uno de los dispositivos de los usuarios. Esta configuración se realizará principalmente en puertos asignados para host realmente críticos.

Se determinará que sólo un equipo con determinada dirección MAC se conecte al puerto asignado del Switch, si algún dispositivo no autorizado se conecta al puerto, este se apagará inmediatamente y su activación se tendrá que hacer manualmente por el administrador de red. De esta manera, además de garantizar que, tanto un servidor de red o un equipo crítico utilizan una dirección IP por medio de DHCP y además sólo un puerto de switch podrá ser utilizado por ese equipo.

El sistema operativo Cisco IOS permite la configuración de la seguridad en los puertos del dispositivo. Esto será a través del comando *switchport port-security*. Cuando se especifique que cierto puerto del equipo será utilizado por una única estación de trabajo, las líneas de configuración serán las siguientes:

```
interface <TIPO_INTERFAZ><SLOT><PUERTO>
 switchport access vlan <IDENTIFICADOR_VLAN>
 switchport mode access
 switchport port-security
 switchport port-security maximum 1
 switchport port-security mac-address <DIRECCIÓN_MAC_EQUIPO>
 switchport port-security violation shutdown
!
```

El puerto al que se le configure la seguridad debe de estar configurado como puerto de acceso de manera estática con el comando *switchport mode access*, ya que de manera predeterminada se encuentra en modo de *dynamic auto*, es decir, si el puerto no se configura y se conecta a un puerto troncal de otro Switch, este puerto actuará como troncal.

Las líneas de configuración anteriores definen la seguridad del puerto para un host con determinada dirección MAC. Si un host distinto al que se ha establecido se conecta al puerto, este último se deshabilitará y tendrá que ser habilitado de manera manual por el administrador de la red.

Con el comando *switchport port-security* se habilitará la seguridad en el puerto. Con ese mismo comando, se define un máximo de direcciones que serán permitidas en el puerto, en este ejemplo se determinó una sola dirección *switchport port-security maximum 1*. Se especifica la dirección física del equipo al que se permitirá el acceso y el modo de actuar de la interfaz en caso de cometerse una violación a la seguridad, con el comando *switchport port-security violation shutdown* se especifica que se apague en caso de infracción.

La manera para verificar que la seguridad ha sido habilitada en un puerto determinado se muestra a continuación:

```
switch#show port-security interface FastEthernet 0/10
      Port Security              : Enabled
      Port Status                : Secure-up
      Violation Mode             : Shutdown
      Aging Time                 : 0 mins
      Aging Type                 : Absolute
      SecureStatic Address Aging : Disabled
      Maximum MAC Addresses      : 1
      Total MAC Addresses        : 1
      Configured MAC Addresses   : 1
      Sticky MAC Addresses       : 0
      Last Source Address:Vlan   : <DIRECCIÓN_MAC>:<VLAN>
      Security Violation Count   : 0
```

Para e puerto FastEthernet 0/10 se ha habilitado la seguridad. En estado del puerto es activo seguro (Secure-up). El modo de violación (Violation Mode) indica la manera en que actuará el puerto en caso de detectarse una quebrantamiento a la seguridad del puerto, en este caso que un host con una dirección MAC distinta a la especificada el puerto se apagará de manera automática.

En caso de presentarse una violación en el puerto, la interfaz se apaga. Para poder observar lo anterior, se muestran las siguientes salidas de comando aplicadas a un puerto en el que no se cumplió con el número máximo de direcciones permitidas el estado de apagado del puerto.

```
switch#show port-security interface FastEthernet 0/10
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000A.F324.0BC4:200
Security Violation Count   : 1
```

Al cometerse una violación a la seguridad del puerto, el estado del mismo pasa de *Secure-up* y al *Secure-shutdown*. En el ejemplo anterior se muestra el estado de la seguridad de un puerto que ha sido violado. El estado de la interfaz pasó de *Secure-up* a *Secure-shutdown*, es decir, se ha apagado la interfaz.

Muchos de los puertos que deben configurarse de esta manera son los que pertenecerán a los equipos de los administradores, ya que tanto la dirección IP y el puerto deben de ser los mismos en la mayoría de las ocasiones ya que habrá listas de control de acceso que no permitirán que cualquier dispositivo logre la gestión de los equipos de la red.

También es importante que los puertos del switch que no se utilizan se apaguen como medida de seguridad ya que cualquier host no autorizado en la red podría conectarse a un puerto disponible del switch y por medio del servicio de DHCP recibir una dirección IP que le permita la salida a Internet y el uso de los recursos de la red sin permiso.

3.6 Gestión de los dispositivos de red a través de SNMP

Es importante tener monitoreada la red, principalmente los dispositivos que tienen un papel clave en la tarea de brindar un servicio. Los Routers en cada uno de los planteles, así como el Router principal necesitan ser monitoreados y detectar cuando se generen problemas.

Para dicha tarea, se ha elegido el protocolo por excelencia utilizado para la gestión de los recursos de los dispositivos, se trata del Protocolo Simple de Administración de Red, SNMP por sus siglas en inglés. Este es usado para administrar dispositivos (Routers, switches, servidores, etc.) en una red. SNMP permite al administrador de red consultar el estado actual de algún dispositivo, colectar datos para análisis y razones históricas, y hacer los cambios en la configuración de ser necesario. SNMP también a un dispositivo el envío de alarmas al agente de monitorización para alertar al administrador y resolver el problema lo más rápido posible.

SNMP es un protocolo de capa de aplicación desde el punto de vista del modelo de capas de TCP/IP que fue diseñado para el intercambio de información para la administración de los recursos de los dispositivos de red, surgiendo los conceptos de agentes y de administrador.

El agente administrador obtiene información y la recopila a través de objetos *MIB* (Management Information Base, Base de información de administración) en el que cada uno de los equipos en el grupo de gestión envía información acerca de su estado.

Los elementos clave en un entorno de gestión sobre SNMP son los que se mencionan a continuación:

- ***Agente administrador de red***: Este es el equipo que pregunta sobre el estado de los agentes de la red. Esto lo hace a través de solicitudes específicas. Una de sus características importantes es que reside en un equipo de cómputo con una cantidad suficiente de memoria RAM, misma que utiliza para el almacenamiento de los estados de cada uno de los agentes que le han brindado información.

  A su vez, este dispositivo tiene la capacidad de mostrar los resultados de forma gráfica y de una manera entendible en la que este desmenuza cada uno de los MIBs que ha generado.

- ***Agente gestionado***: Estos son los equipos que se buscan administrar y proporcionan información sobre el estado de sus componentes al agente administrador. Estos agentes pueden ser cualquier tipo de dispositivo, como Routers, Switches, servidores, etc., que tienen habilitado y configurado el protocolo de SNMP para que envíen información sobre su estado al agente administrador.

  Entre la información que se puede almacenar en las MIBs, se encuentran las siguientes:
  - Número de ciertos mensajes de error generados en el dispositivo.
  - Total de información enviada y recibida a través de sus interfaces.
  - Componentes del dispositivo que han caído y las que se han activado.
  - Estado de los discos duros.
  - Estado del procesador.

  Cuando los agentes gestionados reciben una petición del agente administrador, estos responden enviando la información que se les solicita.

- ***Base de Información de Administración***: Estos son empleados para el almacenamiento estructurado de los elementos que integran la red.

  Hay tres tipos de MIB, y son:

- MIB estándares.
- MIB experimentales (se encuentran en fase de desarrollo).

- MIB privadas (hechas para dispositivos de ciertos fabricantes).

  Todos los valores en la MIB son la colección de valores que han surgido de la petición de información entre el agente administrador y los agentes gestionados.

- Comunicación del protocolo de administración de red: Existen dos formas en las que administradores y agentes se comunican:
- Modo petición – Respuesta: En esta el dispositivo administrador envía una petición de información al agente gestionado para que este último le envíe información.
- Modo de notificaciones: En este modo, el agente envía información extraordinaria al administrador sólo en casos excepcionales, en los cuáles, de inmediato se modifican los MIB correspondientes.

Los mensajes de administración de SNMP se clasifican en tres grupos:

- Lectura: Los administradores reciben información de los agentes para su almacenamiento en las MIBs correspondientes.
- Escritura: Es la capacidad de modificación de objetos administrados en un agente actuando sobre el equipo administrado.
- Notificaciones: El agente envía información al administrador en caso de ocurrir un problema en el equipo.

En la siguiente tabla se mostrarán los siete mensajes utilizados en SNMP:

Tipo de mensaje SNMP	Emisor-Receptor	Descripción
GetRequest	Administrador – Agente	Obtener el valor de una o más MIBs
GetNextRequest	Administrador – Agente	Obtener el valor del siguiente dato en la MIB en una lista
GetBulkRequest	Administrador – Agente	Obtener el valor en un bloque grande de datos
InformRequest	Administrador – Agente	Informa a una entidad administradora remota de los valores MIB remotos de su acceso.
SetRequest	Administrador – Agente	Establece el valor de una o más estancias MIB
Response	Administrador – Agente o Agente – Administrador	Respuesta a un GetRequest, GetNextRequest, GetBulkRequest, SetRequest e InformRequest
SNMP trap	Agente – Administrador	Informe al administrador de un evento excepcional.

Tabla 16. Tipos de mensajes en SNMP.

En la red del IEMS en la red actual y durante el proceso de mejora continua, es necesaria la monitorización de los dispositivos y tomar medidas en caso de presentarse algún problema en alguno de los dispositivos. Hay diversas opciones para poder realizar esto, sin embargo, muchas de ellas son muy costosas, pero demasiado útiles para su fin, por ejemplo, SolarWinds que desarrolla varias herramientas para el monitorización, detección, gestión y supervisión de redes. Sin embargo, es una buena opción la utilización de herramientas libres como son los servidores de Nagios o Cacti.

En este documento no se tratará el desarrollo, instalación y puesta en operación de alguno de estos servicios, pero se mencionarán debido a que son de vital importancia en cualquier red de datos para la monitorización de los recursos.

Nagios es un sistema para monitorizar redes de datos y es de código abierto (Open Source) que tiene la capacidad de vigilar hardware (dispositivos) y servicios de software que se especifiquen en su configuración,

generando alertan en caso de que los comportamientos no sean los que se desean. Entre los servicios que pueden monitorizarse a través de un servidor nagios son los siguientes: SMTP, POP3, HTTP, NTTP, ICMP, SNMP, hardware de dispositivos, como son cargas de procesador, uso de discos duros, archivos de registro de los equipos, y la posibilidad de realizar monitorizacións remotos a través de túneles SSL o SSH.

En la red del IEMS se implementarán servidores de SNMP que serán los agentes administradores que presentarán la información de los dispositivos de red que se instalarán en la red. Los dispositivos a monitorizar son Routers de salida de cada uno de los planteles y switches que estén gestionados, así como el Router-on-a-stick que d salida a todos los planteles de la institución.

A continuación se presenta el procedimiento que se llevará a cabo para la configuración y habilitación de SNMP en un dispositivo de red de la marca Cisco®. Entiéndase que esta sección del documento se aplicará cuando se esté realizando el proceso de mejora y los servidores de monitorización están instalados y funcionando, listos para realizar peticiones de información.

Antes que nada, es primordial tener el direccionamiento de los equipos servidores de SNMP, estos pueden ser desde uno a más dispositivos. Esto es importante para la realización de listas de acceso en los dispositivos de red para permitir sólo a los equipos administradores la realización de peticiones.

```
ip access-list standard Servidores_SNMP
      permit Dirección_IP_de_servidorSNMP_1
      permit Dirección_IP_de_servidorSNMP_2
      permit Dirección_IP_de_servidorSNMP_n
```

Esta lista de control de acceso llamada "*Servidores_SNMP*" permitirá que sólo los agentes administradores de SNMP tengan acceso a la comunidad de SNMP de los dispositivos, las direcciones IP se listan en la ACL. De manera predeterminada, cuando se configura SNMP en un dispositivo de cualquier fabricante, estos utilizan como autenticación un nombre de comunidad, que de manera predeterminada se llama "public". Esta información cuando es enviada entre los dispositivos agentes y el agente administrados, se envían sin cifrar, un gran problema de seguridad, debido a que la información que se transmite por SNMP describe en gran parte cual es la infraestructura de la red de datos y en las manos equivocadas, es un gran problema. Por esa razón, aquí se describirá la forma en que se configurará un dispositivo con una comunidad que no es la predeterminada, y el uso de listas de acceso.

Determinado esto, se configura la comunidad en el dispositivo:

```
Router(config)#snmp-server community iems_gestion RO Servidores_SNMP
```

En la línea de comando anterior se determina el nombre de la comunidad, en este documento se propone el nombre de "Iems_gestion", pero este puede ser un nombre que elija el administrador de red. Las letras "RO" son de *Read-Only* que determina que la información que se compartirá es sólo de lectura. De esta manera y el no usar una comunidad de RW (Read-Write, Lectura y escritura), no se permite que SNMP tenga la capacidad de realizar cambios en los equipos, sólo será información de consulta que se proporcionará. Esta comunidad de SNMP será accesible a los equipos en la lista de control de acceso "*Servidores_SNMP*" y así evitar que cualquier equipo en la red pueda generar una petición de información al dispositivo.

El paso siguiente es indicarle al equipo la dirección IP del agente administrador, puede ser uno o más, mismos que fueron enlistados en la lista de control de acceso.

```
Router(config)#snmp-server host Dirección_IP_de_servidorSNMP_1 iems_gestion
Router(config)#snmp-server host Dirección_IP_de_servidorSNMP_1 iems_gestion
Router(config)#snmp-server host Dirección_IP_de_servidorSNMP_1 iems_gestion
```

En las líneas anteriores se indica al dispositivo las direcciones IP de los agentes administradores, así como la comunidad en la que van a trabajar.

Para habilitar que el dispositivo envíe información que se requiere, se habilitará el envío de *traps*, esta es la información que se le solicite desde el agente administrador.

```
Router(config)#snmp-server enable traps
```

Sin embargo, se puede delimiter al equipo el envío de ciertos traps y no de varias variables. La línea anterior habilita al equipo a enviar cualquier tipo de información que se le requiera, pero puede delimitarse qué tipo de información se enviará y el envío de traps de forma individual, esto anteponiendo el comando *snmp-server enable traps entity*.

```
Router(config)#snmp-server enable traps entity
Router(config)#snmp-server enable traps cpu
Router(config)#snmp-server enable traps memory
Router(config)#snmp-server enable traps eigrp
Router(config)#snmp-server enable traps config
Router(config)#snmp-server enable traps tty
Router(config)#snmp-server enable traps linkdown
Router(config)#snmp-server enable traps linkup
...
```

El agente administrador, en este caso Nagios, es un equipo que tiene instalado el servicio de Nagios, MySQL como su gestor de base de datos, un servidor web (usualmente en Apache) para el despliegue de la información a los administradores de red, y por supuesto, el servicio de SNMP como servidor para el envío de las solicitudes de información.

Para la monitorización de los equipos, se define un archivo de configuración definiendo los nombres de los dispositivos a monitorizar, su direcciones IP, nombre de comunidad de SNMP, parámetros a explotar, entre otras cosas. En la red del IEMS se configurará un archivo para los, uno para los switches de los planteles, un archivo para los servidores web, entre otros servicios, el que interesa en esta sección son los equipos de red.

El archivo sería como el siguiente *routers.cfg*:

```
define host{
        use         generic-switch
        host_name   router-principal
        alias       router-principal
        address     <dirección_ip_router>
        hostgroup   routers_iems
}
```

En las líneas anteriores especifican un equipo a monitorizar, en las líneas anteriores se definió al Router-on-a-stick que da acceso a los planteles, este pertenecerá a un grupo de equipos al que se le llamará *routers_iems*.

```
define hostgroup{
        hostgroup_name  routers_iems
        alias           Routers IEMS
}
```

Los anteriores comandos definen el grupo en el que otros dispositivos pueden unirse para ser monitoreados y un nombre de Alias, con el cuál se identificarán en la interfaz gráfica Web de los administradores.

```
define service{
        use         generic-service
        host_name  router-principal
        service_description    Uptime
        check_command   check_snmp!-C iems_gestion -o sysUpTime.0
}
```

Estas líneas definen el servicio que se va a monitorizar del equipo que se definió en las líneas anteriores. Este bloque de configuración del archivo routers.cfg monitorea el tiempo que lleva encendido el equipo. Se indica a Nagios que envié una petición al agente por medio de un *check_snmp!* a la comunidad *iems_gestion* (que está configurada en el Router o conjunto de Routers) solicitando el parámetro *sysUpTime* que, en SNMP, es el tiempo que lleva encendido el dispositivo.

De esta manera se deben de definir todos los parámetros que se desean monitorizar. Los *check_command* de Nagios pueden definirse para solicitar un solo parámetro a monitorizar como el *sysUpTime*, o un conjunto de parámetros, pero esto a través medio de números ya definidos por SNMP para cada medida monitoreable, hace la consulta más rápida y más eficiente.

```
define service{
        use generic-service
        host_name router-principal
        service_description OID Uptime
        check_command check_snmp!-C public -o .1.3.6.1.2.1.1.3.0
}
```

4

Pruebas de validación y resultados

4.1 Pruebas de validación de la implementación de la red por puertos extendidos

El presente capítulo está destinado a la definición de una matriz de pruebas y verificación de la implementación de los diferentes puntos tratados a lo largo de este documento.

En las empresas de tecnología, es una práctica habitual realizar la creación de matrices de pruebas cuando se va a implementar una solución, estas ayudan a detectar los puntos clave en el que es necesario validar que cada tarea planeada se ejecute de manera satisfactoria, y tomar las medidas necesarias en caso de que no se esté cumpliendo con lo esperado.

Se describen las consideraciones que deben ser tomadas en cuenta con respecto a los dispositivos que se integran a la red y la verificación de la calidad del servicio brindado a los usuarios por la infraestructura, de funcionamiento esperado contra funcionamiento real, toma y ejecución de solicitudes por parte de los miembros de la red, así como respuestas en caso de fallas e incidentes.

Una de las situaciones en las que se encuentra actualmente el IEMS es la siguiente: Varios de los planteles tienen instalado un Router de salida sobre un dispositivo con PfSense corriendo sobre ellos, el Router principal que une a todos los planteles con los enlaces de salida a Internet es un dispositivo Cisco® con múltiples rutas estáticas hacia las redes locales de los planteles para que estos tengas comunicación entre si y puedan compartir aplicaciones y servicios a un nivel local y privado dentro de la organización. Asimismo, existen algunos planteles que aún utilizan la red pública de Internet para sus necesidades, es necesaria la inclusión de estos al esquema que se ha desarrollado para que toda la infraestructura de la institución se encuentre viajando de manera segura y privada a través de los enlaces Lan-to-Lan.

La principal desventaja que se tiene con los dispositivos que hoy en día se encuentran instalados en los planteles es que, a cualquier cambio en la red, ya sea debido a un cambio de direccionamiento, integración de un nuevo plantel o pérdida de alguno de los planteles por causa de un incidente, la respuesta al restablecimiento del servicio será lento, la convergencia se vuelve tardía y se tiene que configurar de manera manual el cambio en la red, por mínimo que sea, lo cual, puede provocar algún error en la configuración que retrase la puesta en operación. Por eso mismo, es necesaria la inclusión de dispositivos de red que soporten protocolos de ruteo dinámico y brindar tiempos de convergencia menores y una manera automática de plasmar los cambios de la red informando a todos los dispositivos las modificaciones o inclusión de equipos nuevos a la red.

La matriz de verificación se ejecutará para identificar los puntos a considerar en la implementación y activación de cada una de las acciones sobre la red en cualquiera de sus puntos y la validación de que el servicio está funcionando.

Este capítulo del documento debe ser utilizado en cualquier situación en la que se encuentre la red durante su crecimiento y evolución para su validación correcta. Se debe utilizar desde sus inicios con la instalación de los Routers de salida sobre PfSense en cada plantel y su conexión al Router principal en las oficinas centrales por medio de los enlaces Lan-to-Lan, en la integración a la red de los planteles que aún se encuentran aislados de la red principal. Migración de los Routers PfSense en cada plantel por dispositivos de alguna marca comercial grande en el mercado de los dispositivos de red, tal como es el caso de Cisco®. Implementación del protocolo de ruteo dinámico y pruebas de convergencia de la red. Instalación y puesta en marcha de firewalls, servidor proxy, IDS, implementación de la seguridad en la red en dispositivos fundamentales de la red, entre otros escenarios posibles.

Se recomienda que cada uno de los movimientos que se mencionan en este documento sean analizados antes de la ejecución y se programe una prueba piloto en una ventana de mantenimiento nocturna o en algún día en el que no haya actividad en la red como días festivos, para no afectar a los usuarios y tomar en cuenta tiempos de ejecución e

identificar puntos críticos de la implementación que se habían tomado en cuenta y los que no se habían identificado por alguna cuestión no esperada.

4.2 Matrices de Verificación

A continuación se presentarán diversas matrices de verificación para validar el servicio de red entre los planteles del IEMS, funcionamiento del protocolo de ruteo dinámico, migración de plataformas en los equipos de cada plantel, pruebas de conectividad, pruebas en la seguridad de los equipos, inclusión de un nuevo plantel, respuesta a fallas.

4.2.1 Instalación de equipo PfSense y conexión a enlace L2L

En la siguiente matriz de verificación se toman en cuenta las pruebas que se deben de tomar en cuenta durante la instalación de un Router de salida sobre PfSense.

Tabla 4.1. Prueba y validación de conectividad.

Concepto	Criterio de verificación
Verificar que el enlace L2L físico provisto por el proveedor está en funcionamiento y la interfaz del equipo ya está activa. Asimismo, establecer l conexión a la red LAN.	Entrar al equipo y verificar que ambas interfaces están en estado activo “active”. De no ser así, en el caso del enlace L2L, realizar pruebas con el proveedor, en el caso de la interfaz hacia la LAN, verificar el cableado. Configurar el direccionamiento asignado para ambas interfaces.

- **Prueba de conectividad**

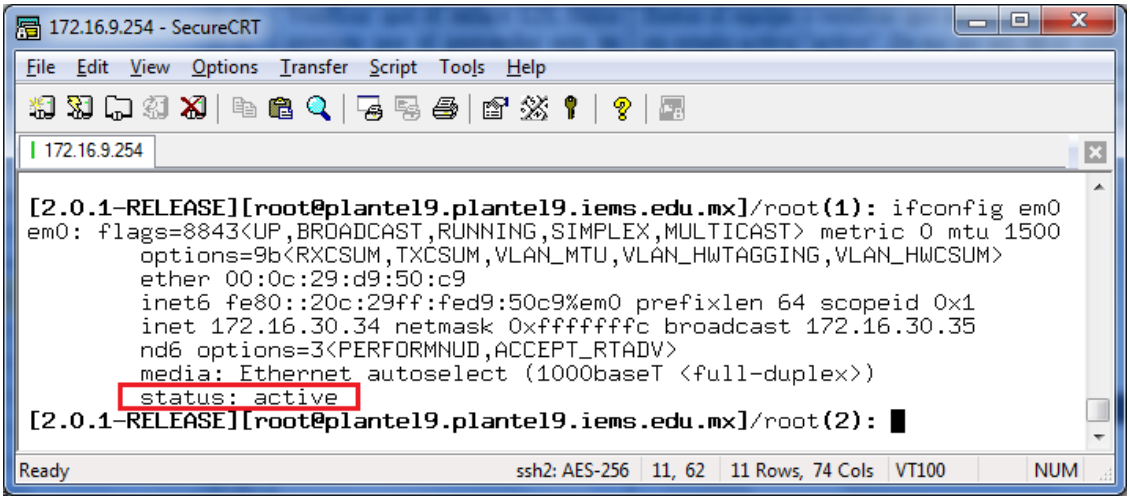

Figura 4.71. Verificación de interfaz WAN del Router del Plantel 9

Tabla 4.2. Prueba y validación de conectividad.

Concepto	Criterio de verificación
Comprobar que se tiene la configuración asignada al plantel que se está activando en el Router de enlace on a stick. Esta configuración debe de incluir el direccionamiento asignado al enlace L2L.	Entrar al Router principal y verificar que se ha configurado la subinterfaz correspondiente al plantel, asimismo, corroborar que se tiene configurada sobre la VLAN que ofrece el proveedor para el enlace L2L correspondiente. Verificar que se tiene conectividad de extremo a extremo a través del

	comando PING. En caso de no existir conectividad, verificar que el direccionamiento esté configurado bien y sea el correcto, en caso contrario, revisar el medio de transmisión con el proveedor.

- **Prueba de conectividad**

```
 7) Ping host

Enter an option: 7


Enter a host name or IP address: 172.16.30.33

PING 172.16.30.33 (172.16.30.33): 56 data bytes
64 bytes from 172.16.30.33: icmp_seq=0 ttl=64 time=47.378 ms
64 bytes from 172.16.30.33: icmp_seq=1 ttl=64 time=0.203 ms
64 bytes from 172.16.30.33: icmp_seq=2 ttl=64 time=0.201 ms

--- 172.16.30.34 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.201/15.927/47.378/22.239 ms

Press ENTER to continue.
```

Figura 4.72. Ping al Router On a Stick de enlace.

Tabla 4.3. Prueba y validación de servidor DHCP dinámico.

Concepto	Criterio de verificación
Verificar la configuración del servidor de DHCP del dispositivo PfSense y su asignación de direccionamiento por medio de la confirmación de comunicación entre la red local y el Router PfSense.	Entrar al Router PfSense y verificar la configuración del servicio de DHCP. Confirmar que los hosts en la red local se les ha asignado el direccionamiento dentro del pool configurado en el Router. Lanzar un comando PING entre el host y el Router PfSense para comprobar comunicación, en caso de ser fallido, revisar que los parámetros que han sido asignados por DHCP son los correctos y modificar en caso de error.

- **Prueba de asignación de IP y de conectividad**

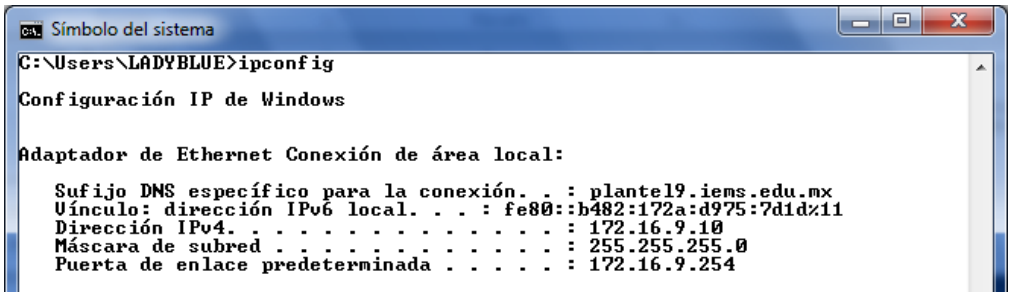

Figura 4.73. Asignación de IP por medio de servidor DHCP

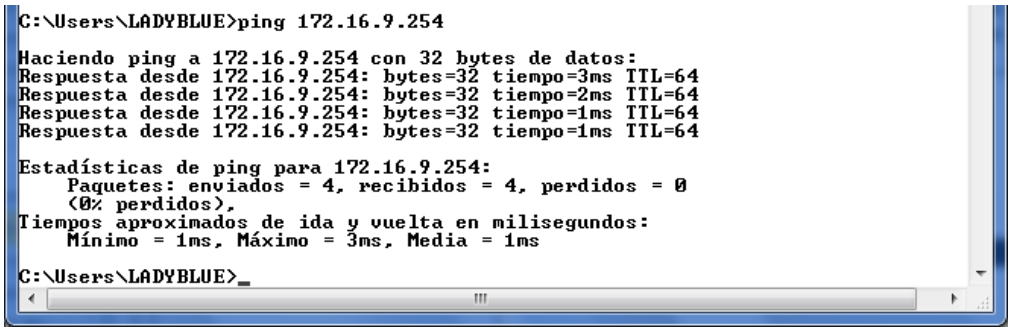

Figura 4.74. Equipo de la red local que recibe IP del servidor DHCP.

Tabla 4.4. Prueba y validación de ruteo entre VLAN.

Concepto	Criterio de verificación
Inspeccionar en el Router principal que las rutas estáticas a los planteles y la ruta predeterminada a Internet se encuentren configuradas.	Entrar al Router de acceso y verificar que todas las rutas estáticas a los planteles del IEMS están configuradas, así como la ruta hacia los enlaces a Internet. En uno de los host de la LAN enviar un PING a cualquier otro host en otro plantel, así como un PING hacia una dirección de Internet. En caso de ser negativa la prueba, verificar que las líneas estén bien configuradas. Además, verificar que se tiene configurada la ruta pro default sobre la interfaz que apunta hacia las salidas de Internet.

- **Prueba de conectividad**

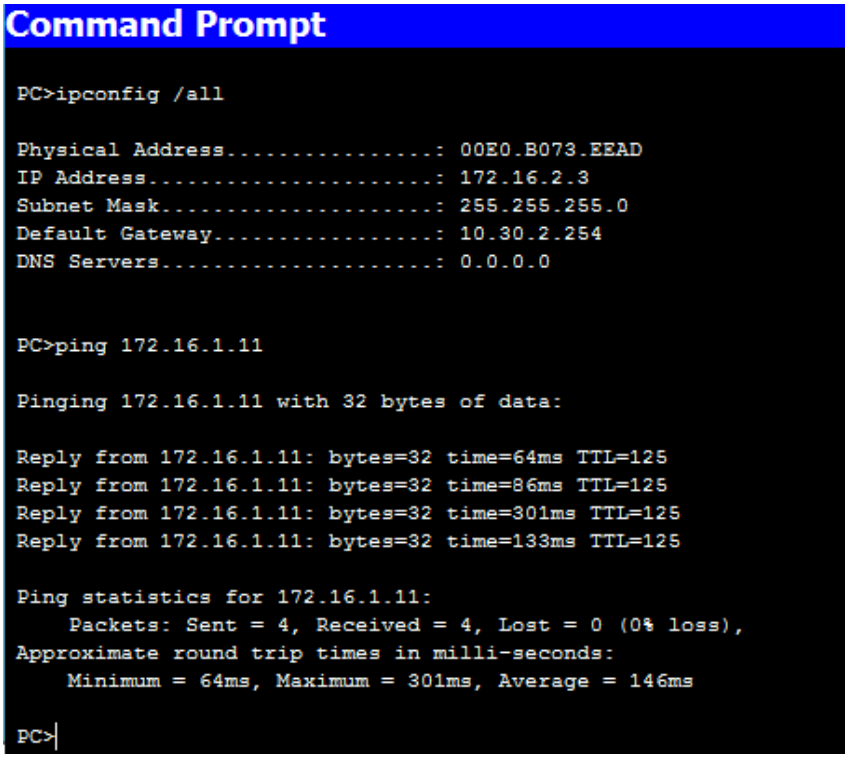

Figura 4.75. Conectividad de host de plantel 2 a plantel 1

Tabla 4.5. Prueba y validación de DHCP estático.

Concepto	Criterio de verificación
En el caso de las asignaciones DHCP por medio de dirección MAC, verificar que los equipos estén tomando los parámetros correctos que les permitan la salida hacía Internet.	Revisar que los equipos servidores, impresoras, teléfonos IP, entre otros, están tomando las direcciones IP por medio de su dirección MAC. Inspeccionar que se tiene comunicación con esos equipos y que están en funcionamiento. Varios de esos equipos no importa si salen a Internet, son sólo de uso local.

4.2.2 Migración de equipo PfSense a un Router comercial

A continuación se presenta la matriz de prueba de los aspectos que se deben de tomar en cuenta durante la migración de plataforma en alguno de los planteles, a un Router del mercado de dispositivos de red, por ejemplo, un equipo de la marca Cisco® que cumpla con las necesidades del nodo en el que se realice el cambio. En este caso se considera que el protocolo de ruteo dinámico aún no se implementa en la red.

Tabla 4.6. Prueba y validación de parámetros de red.

Concepto	Criterio de verificación
Verificar que los parámetros de red que se han establecido para el nuevo dispositivo son los mismos que se están considerando en la nueva plantilla de configuración.	Revisar el documento de implementación y verificar que en la configuración se tomen en cuenta todos los parámetros de red del dispositivo PfSense actual, tal es el caso de direcciones IP de las interfaces, pooles de DHCP, nombre del dispositivo, descripciones sobre interfaces, dirección IP del Gateway.

Tabla 4.7. Validación de configuración

Concepto	Criterio de verificación
Confirmar la configuración del nuevo dispositivo se haya realizado.	Antes de instalar el dispositivo, entrar a la línea de comandos a través de una conexión fuera de banda (a través del cable de consola RJ45- DB9) para verificar que los parámetros que están definidos en el documento de implementación han sido configurados.

Tabla 4.8. Prueba y validación de conectividad y servicio de DHCP

Concepto	Criterio de verificación
Se retira el Router PfSense y se instala el nuevo dispositivo. Verificar que levanten las interfaces sin problemas y haya conectividad con los extremos.	Entrar al dispositivo y comprobar que las interfaces hayan levantado, en caso de que no lo hagan, verificar que se ha incluido el comando “no shutdown” en los puertos. En caso de no ser ese el problema, verificar que no se han dañado conectores que van hacia la LAN y hacia el enlace L2L. Verificar que los equipos de la LAN están recibiendo la IP correspondiente de los pooles de DHCP configurados, lanzar comando PING para la verificación de la comunicación entre LAN y equipo de salida. En caso de no ser exitosos, verificar que la configuración realizada en las interfaces es la que se estableció en el documento, validar que sea información correcta.

Tabla 4.9. Prueba y validación de ACL en Routers Cisco®

Concepto	Criterio de verificación
Verificar que la configuración de las listas de acceso está ejecutándose.	Validar que las listas de acceso están haciendo su trabajo. Estás listas de control de acceso son para permitir o denegar la entrada vía TELNET o SSH a la línea de comandos del dispositivo para su administración. Sólo equipos con direcciones IP permitidas deben de acceder, para otra IP debe de ser negado. En caso de no funcionar lo anterior, validar que se ha aplicado la ACL a la línea de VTY o identificar posibles errores en las direcciones especificadas en la lista de acceso.

- **Pruebas de ACL de acceso vía remota**

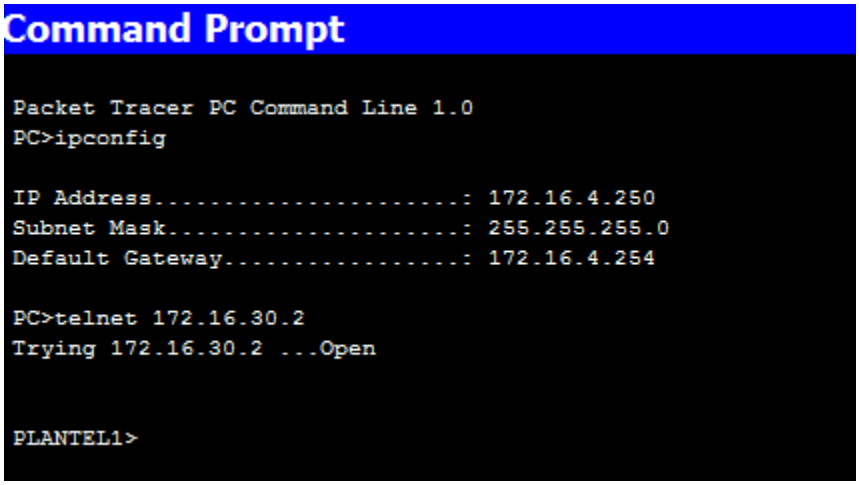

Figura 4.76. Prueba de acceso vía telnet desde equipo administrador

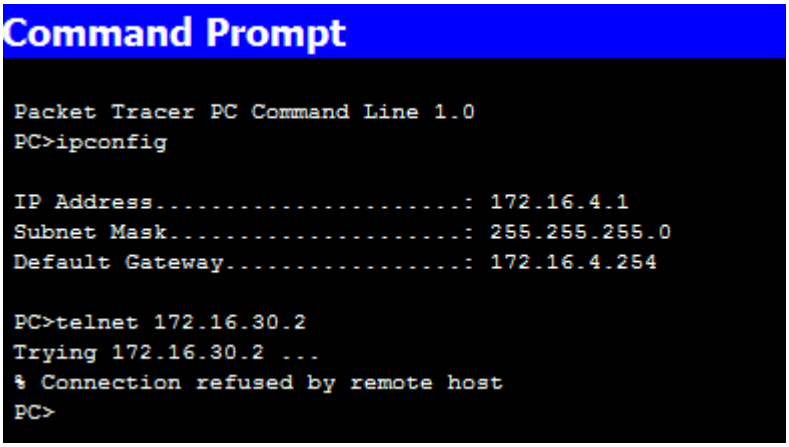

Figura 4.77. Prueba de acceso vía telnet desde equipo de usuario normal

Tabla 4.10. Prueba y validación de conectividad a Internet.

Concepto	Criterio de verificación
Validar que los usuarios están navegando en internet.	Entrar a un equipo dentro de la red local, verificar que este tiene comunicación con la dirección IP para la red local en el Router principal configurada en la interfaz correspondiente, asimismo, verificar que se tiene salida hacia Internet. En caso de no ser así, comprobar que las direcciones IP de salida se encuentran configuradas correctamente.

4.2.3 Configuración del protocolo de ruteo dinámico EIGRP

A continuación se presenta la matriz de validación para la validación del funcionamiento del protocolo de ruteo dinámico EIGRP.

Tabla 4.11. Prueba y validación de protocolo de ruteo dinámico

Concepto	Criterio de verificación
Validar que la configuración de EIGPR se encuentre en todos los equipos considerados para participar en el dominio de ruteo.	Entrar a cada uno de los dispositivos en los planteles y verificar que sólo la interfaz que está conectada al enlace L2L se encuentra configurada para compartir información de ruteo. Asimismo, validar que todas las redes configuradas en el dispositivo se encuentren anunciadas en el proceso de ruteo.
Comprobar que la red se actualiza dinámicamente a través del protocolo de ruteo EIGRP.	Acceder a todos los Routers de la red que tienen activado el protocolo de ruteo dinámico y verificar que todos estos tenga sus tablas de ruteo completas, es decir, cuenten con todas las rutas hacia las redes locales y las redes de cada uno de los enlaces L2L.
Verificar la conectividad con Internet.	Entrar a algún host dentro de las redes locales y probar la conectividad con Internet por medio de un PING a una dirección externa o accediendo través del navegador a una página web.
Revisar rutas estáticas en el Router principal.	Entrar al Router Principal y revisar que no existe ninguna ruta estática configurada, a excepción de la ruta estática por default con la interfaz que apunta hacia a las salidas a Internet de la red institucional. En el caso de que todos los planteles aún no se hayan migrado de PfSense a un Router comercial, permanecen las rutas estáticas a esas redes locales.
Revisar la configuración de la autenticación de EIGRP.	Entrar a los Routers que se han configurado para EIGRP y revisar que se tenga aplicada la configuración. Asimismo, verificar que la adyacencia de EIGRP se haya establecido.

4.2.4 Integración de un Router que no soporta la configuración de EIGRP

La siguiente tabla nos explicará los puntos necesarios que hay que tomar en cuenta para la validación de la integración a la red de un dispositivo que no soporte la configuración de EIGRP. Es útil mencionar nuevamente que esta red está diseñada para que funcione en un entorno con dispositivos de la marca Cisco®, razón por la cual se tomó a EIGRP como el protocolo principal para el intercambio de información de ruteo.

Tabla 4.12. Prueba y validación de Router nuevo que no soporta EIGRP.

Concepto	Criterio de verificación
Verificar que en los Routers haya sido ejecutada la configuración correcta.	Entrar al equipo nuevo que se colocará en el plantel y revisar que los parámetros de red hayan sido configurados correctamente. También acceder al Router principal (Router-on-a-stick) y verificar que tenga la configuración adecuada, así como los parámetros correctos.
Validar que entre los dos dominios de ruteo (EIGRP y RIP) haya intercambio de información de ruteo a través de la redistribución.	Entrar al Router-on-a-stick y al Router del plantel que se ha instalado, corroborar que ambos Routers están compartiendo rutas entre los dos diferentes protocolos de ruteo. Se tienen que ver entradas E EX en el equipo On-a-stick.
Comprobar que existe comunicación entre los equipos del dominio de EIGRP con los equipos de la red local del equipo sobre OSPF.	A través de los equipos de las redes LAN, verificar que los host de la red local del Router que se ha integrado se comunican con otros host en la red local de algún otro plantel. En caso de no ser exitosa la prueba, revisar de nueva cuenta los parámetros configurados.

4.2.5 Prueba de la seguridad: ACLs, puertos en los switches y firewalls

Si el proceso de mejora aún no se ha llevado a cabo, es necesario tener dos matrices de verificación, una para la prueba de los firewalls que controlan el acceso y salida a las redes, y otra que prueba las ACL en los Routers que se han instalado en la mejora de la red con la implementación de los nuevos Routers.

- Matriz de verificación para Firewall

Tabla 4.13. Prueba y validación de firewall

Concepto	Criterio de verificación
Verificar el direccionamiento de que se utiliza en las reglas de filtrado en el archivo *pf.conf* sea el indicado.	Entrar al equipo OpenBSD que está al borde de la red y verificar que el direccionamiento que se considera para los equipos de administración está bien los rangos, así como el direccionamiento general para las salidas a internet (puertos 80 y 443 para http y https respectivamente).
Revisar que Packet Filter en lo equipos OpenBSD está habilitado y está filtrando los paquetes siguiendo las reglas que se le han configurado.	Utilizar un equipo con una dirección IP que corresponde al grupo de administración y acceder al Router PfSense de salida por medio de SSH o HTTP. Asimismo, estos equipos tienen acceso a cualquier protocolo hacia Internet, comprobar que FTP es accesible, por ejemplo. Este acceso está restringido a cualquier otro usuario. Sólo HTTP y HTTPS están permitidos, comprobarlo, así como verificar que FTP es inaccesible.

- Matriz de Verificación de Listas de Control de Acceso en los Routers.

Tabla 3.14. Prueba y validación de Listas de Control de Acceso

Concepto	Criterio de verificación
Verificar el direccionamiento de que se utiliza en las líneas de configuración de las Listas de Control de Acceso en el Routers. También verificar que estén correctamente aplicadas a las interfaces correctas.	Entrar al Router y comprobar que el direccionamiento configurado en las ACL estándar 10 con las IP de los equipos administradores en la red de la institución. Esta ACL debe de estar aplicada en la línea de VTY del dispositivo, para su control de acceso vía SSH o Telnet al equipo.
Verificar que la Lista de Control de Acceso en el Router Principal On a Stick para acceso a	Entrar al Router on a stick que da salida a todos los planteles y comprobar que la ACL extendida SERVICIOS_PERMITIDOS tiene

Internet está configurada con el direccionamiento correcto.	configurado el direccionamiento correcto y está aplicada en la interfaz de conexión de salida a Internet. Con un equipo host de la red local probar que se está ejecutando correctamente, asimismo, usar un dispositivo con direccionamiento de administrador para su prueba de acceso total a los puertos de Internet.

- **Prueba de salida de comando**

```
ROUTER#show ip access-lists SERVICIOS_PERMITIDOS
Extended IP access list SERVICIOS_PERMITIDOS
    permit ip 172.16.1.248 0.0.0.7 any (7 match(es))
...
<Se omiten resultados>
...
    permit tcp 172.16.0.0 0.0.255.255 any eq www (7 match(es))
    permit tcp 172.16.0.0 0.0.255.255 any eq 443 (5 match(es))
    permit icmp any any echo (4 match(es))
    permit udp any any eq domain (15 match(es))
ROUTER#
```

- Matriz de Verificación de la seguridad en los puertos del Switch.

Tabla 3.15. Prueba y validación de la seguridad en los puertos del Switch

Concepto	Criterio de verificación
Verificar que la configuración en el puerto específico esté realizada correctamente. Validar con una computadora personal o móvil, identificar su dirección física MAC e incluirla en la configuración. Conectar al puerto y solicitar una dirección IP del servidor de DHCP, ya asignada la IP, enviar un ping al Router de salida o a Internet (esto para agregar la entrada a la tabla de direcciones MAC).	Entrar al Switch y comprobar la configuración realizada con los comandos de validación necesarios. Revisar que el puerto al que se le va a implementar la seguridad se encuentre configurado como puerto de acceso estático. Las configuraciones de seguridad del puerto deben incluir que cuando se produzca una violación al criterio el puerto se apague. Verificar que la dirección MAC que se configuró en el Switch sea la misma a la de la estación de trabajo que se conectará en ese puerto.
Verificar que las configuraciones de seguridad en el puerto están funcionando adecuadamente. Desconectar el equipo que se conectó al puerto del Switch para conectar otro. Al realizar dicha actividad, el puerto debe de apagarse automáticamente.	Verificar que el puerto se apaga al conectar un host con una dirección MAC distinta a la que se configuró para permitir el acceso a la primera computadora.

- **Salida de comando. Verificación de la configuración de la seguridad en el puerto del Switch.**

```
Switch#show port-security interface FastEthernet 0/10
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
```

```
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0009.7C17.3969:200
Security Violation Count   : 0
```

- **Salida de comando. Verificación de la tabla de direcciones MAC.**

```
Switch#show mac-address-table interfaces FastEthernet 0/10
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

 200    0009.7c17.3969    STATIC      Fa0/10
```

- **Salida de comando. Verificación de la penalización por violación al puerto.**

```
switch2#show interfaces FastEthernet 0/10
FastEthernet0/10 is down, line protocol is down (err-disabled)
```

4.2.6 Pruebas al esquema de redundancia

- Matriz de verificación del funcionamiento de las redundancias a Internet.

Para que un plantel tenga redundancia por otra salida a Internet y además realice balanceo de tráfico por ambas, los dos enlaces L2L deben de ser de la misma capacidad para el flujo de tráfico. Asimismo, las conexiones a Internet deben de ser del mismo volumen de datos. Esta característica es muy importante ya que en el caso de que se realice la configuración como se describe en este documento y no se cumplen dichas premisas, existe un esquema asimétrico en el que una salida tiene mayor capacidad de flujo de tráfico de datos que la otra, pero ambas intentan enviar la misma cantidad de datos provocando que el enlace más pequeño pierda parte del tráfico.

En el caso de que las salidas no sean del mismo volumen, la configuración de rutas estáticas es la solución. Estas son rutas estáticas predeterminadas; sin embargo, aquella con la salida al enlace más pequeño tendrá una distancia administrativa mayor a la de 1 para que se prefiera la salida por el enlace de mayor capacidad.

Tabla 3.16. Prueba y validación de salida a Internet por dos enlaces.

Concepto	Criterio de verificación
Verificar los dos enlaces de salida del Router del plantel.	Verificar ambos enlaces y salidas a Internet sean de la misma capacidad, si es así, comprobar que ambos enlaces están trabajando y están intercambiando rutas, entre ellas la ruta predeterminada que en la tabla de enrutamiento debe tener dos entradas con diferente dirección del siguiente salto. En caso de tenerse los enlaces simétricos y no se está aprendiendo la ruta predeterminada, revisar que los Routers en las salidas están generando la ruta.

4.2.7 Pruebas en la red local

- Matriz de validación de redundancia en la Red Local

Tabla 3.17. Prueba de STP y estados de los puertos.

Concepto	Criterio de verificación
Verificar que el esquema de red de switches no excede el diámetro de la red de siete. Habilitar que el protocolo de RSTP sea el que trabaje en la red local. Asimismo, plasmar la red física en un diagrama y detectar posibles loops. Realizada esta actividad, especificar qué caminos entre los switches se desea que se mantengan activos y configurar los dispositivos para que el protocolo RSTP asigne los roles y los estados a los puertos.	Comprobar que todos los switches en la red local están trabajando con el protocolo de RSTP. Realizada la identificación de switches, establecer las prioridades en cada uno de los dispositivos configurando la prioridad más pequeña al switch que se desea participe en el proceso como puente raíz. Determinar si el estado y el rol de los puertos son correctos según la topología y las prioridades establecidas.
Revisar la configuración de los puertos de acceso.	Verificar que los puertos de acceso no pasan por los estados de STP para pasar del estado de bloqueo al estado de enviar en 45 segundos, sino que, por medio a *portfast*.

4.2.8 Prueba del servidor Proxy

Este procedimiento de validación comprueba si el servidor proxy está funcionando como se estableció en los procesos de instalación y configuración. La página web de información de acceso denegado ha sido modificada y colocado una personalizada, a continuación

- Matriz de verificación del funcionamiento de squid.

Tabla 3.18. Prueba y validación de servidor proxy.

Concepto	Criterio de verificación
Verificar que el proxy está habilitado y funcionando.	Entrar al equipo OpenBSD y verificar que el puerto 3128 está abierto y en escucha. De no ser así, ejecutar los comandos para su activación. Asimismo, verificar que Packet Filter tiene habilitada la regla para redirigir el tráfico web al puerto del proxy.

- **Prueba de solicitudes atendidas por el servidor proxy.**

```
#
# netstat -an | grep 3128
tcp        0      0  127.0.0.1.3128         172.16.9.23.35647      ESTABLISHED
tcp        0      0  127.0.0.1.3128         172.16.9.23.39002      ESTABLISHED
tcp        0      0  127.0.0.1.3128         172.16.9.23.33315      ESTABLISHED
tcp        0      0  127.0.0.1.3128         172.16.9.23.33314      ESTABLISHED
tcp        0      0  127.0.0.1.3128         172.16.9.23.38999      ESTABLISHED
tcp        0      0  127.0.0.1.3128         172.16.9.23.38998      ESTABLISHED
tcp        0      0  127.0.0.1.3128         172.16.9.23.38997      ESTABLISHED
tcp        0      0  127.0.0.1.3128         172.16.9.23.38993      ESTABLISHED
tcp        0      0  127.0.0.1.3128         172.16.9.23.38977      ESTABLISHED
tcp        0      0  127.0.0.1.3128         172.16.9.23.35242      ESTABLISHED
tcp        0      0  127.0.0.1.3128         172.16.9.23.33277      ESTABLISHED
tcp        0      0  127.0.0.1.3128         172.16.9.23.33273      ESTABLISHED
tcp        0      0  127.0.0.1.3128         172.16.9.23.34194      ESTABLISHED
tcp        0      0  127.0.0.1.3128         172.16.9.23.34193      ESTABLISHED
tcp        0      0  127.0.0.1.3128         172.16.9.23.34192      ESTABLISHED
tcp        0      0  127.0.0.1.3128         172.16.9.23.34189      ESTABLISHED
tcp        0      0  127.0.0.1.3128         172.16.9.23.48664      ESTABLISHED
tcp        0      0  127.0.0.1.3128         172.16.9.23.56358      TIME_WAIT
tcp        0      0  127.0.0.1.3128         172.16.9.23.50902      TIME_WAIT
tcp        0      0  127.0.0.1.3128         172.16.9.23.35316      TIME_WAIT
tcp        0      0  127.0.0.1.3128         172.16.9.23.58915      TIME_WAIT
tcp        0      0  *.3128                 *.*                    LISTEN
# _
```

Figura 4.78. Conexiones al puerto 3128 de Squid.

- Matriz de verificación de funcionamiento de squid

Tabla 3.19. Prueba y validación de funcionamiento de proxy.

Concepto	Criterio de verificación
Verificar que se está haciendo el filtrado.	Para la realización de esta prueba es necesario que se esté intercambiando de IP el equipo con el que se está realizando la prueba. Verificar que cada uno de los perfiles que se ha definido cumple con las reglas que se establecieron en el archivo de configuración de squidGuard.

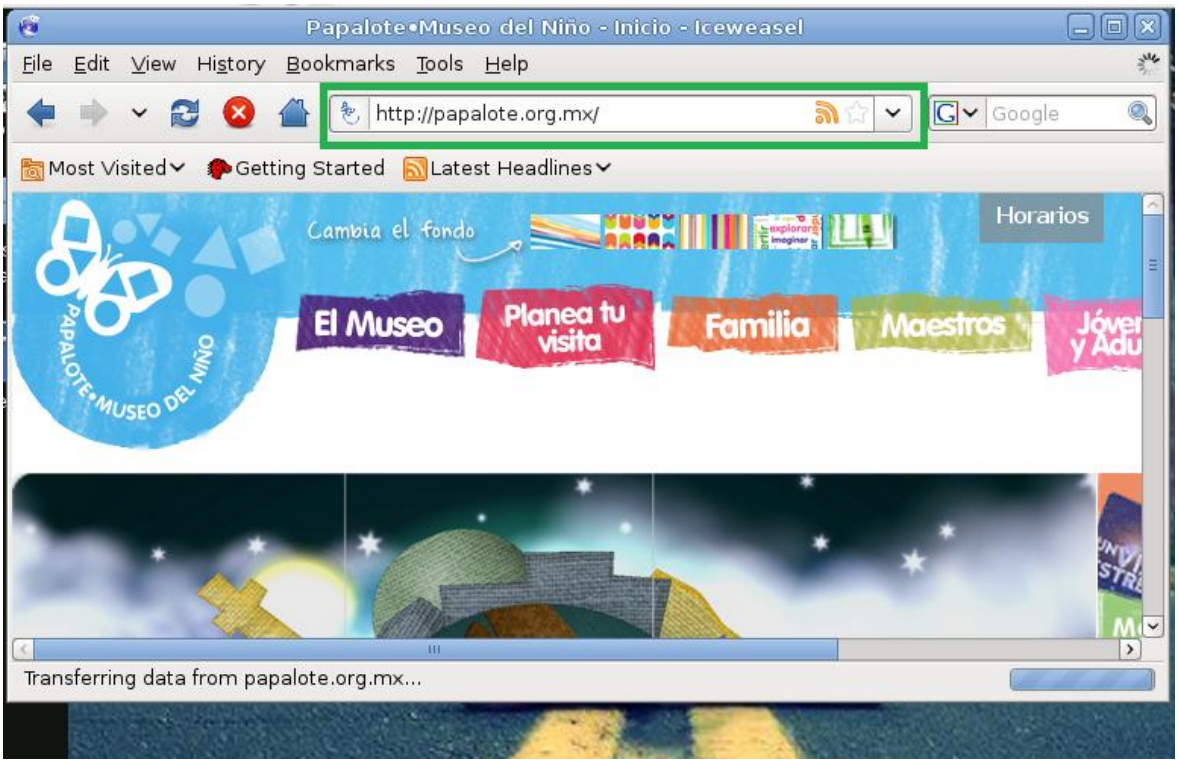

Figura 4.79. Acceso a una página permitida por Squid.

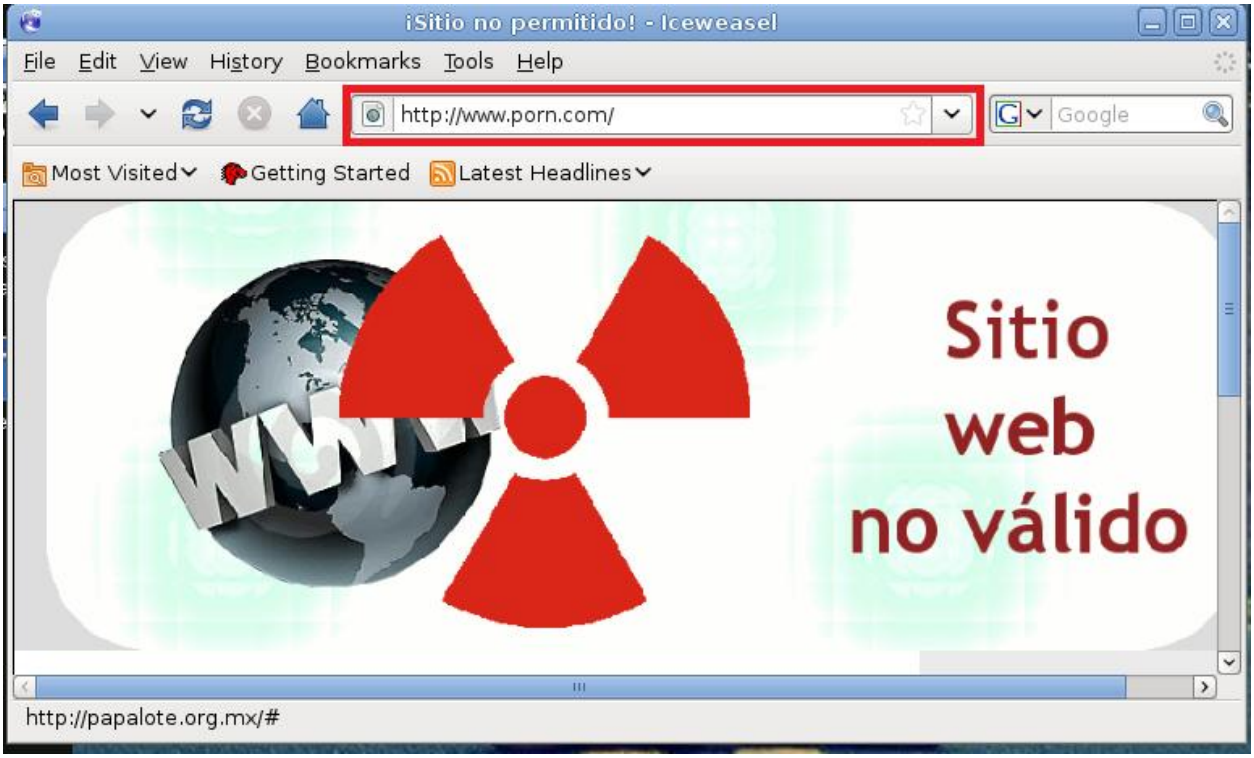

Figura 4.80. Denegación de una página prohibida por Squid.

Figura 4.81. Mensaje personalizado de denegación de acceso a página web.

Resultados

Este trabajo trató del desarrollo de una red por puerto extendido y se dio un documento que explica a detalle la planeación de una red funcional. Además, como se planteó la nueva red, esta puede ser utilizada en cualquier lugar, ya sea educativo nuevamente o en una empresa particular.

Todos los puntos que se desarrollaron pudieron ser planeados, estudiados e implementados a manera de prueba antes de su ejecución final. Asimismo, la mayoría de las tecnologías que se están utilizando en la red del IEMS son libres, tal es el caso de la plataforma PfSense y OpenBSD, mismas que antes de ser implementadas en producción, estás fueron probadas en entornos virtuales.

La mayoría de las pruebas realizadas fueron de conectividad entre los planteles y los dispositivos centrales. Muchos de los problemas que se encontraron durante las pruebas fue que no existía comunicación entre extremos, así que, descartando problemas de configuración o de los equipos de red propios, se determinó que el proveedor de servicios tendría que ajustar algo en sus equipos y así solucionarse.

Otra de las pruebas de conectividad que se han hecho hasta el momento, es la verificar que los equipos o estaciones de trabajo en cada uno de los planteles que actualmente se encuentran en operación tengan salida a Internet sin problema. Por lo que, en ese punto las pruebas van desde los equipos de salida en los planteles, el equipo central y los equipos que le dan salida a la red completa, es decir, routers PfSense y OpenBSD instalados como Router y Firewall respectivamente.

Principalmente, los equipos que se encuentran conectados al proveedor de servicios como el firewall y el Router PfSense las pruebas principalmente en que todas las reglas de filtrado que ese establecieron en el firewall están funcionado en su totalidad, y la verificación de que el Router PfSense está realizando la traducción de direcciones. La traducción de direcciones (NAT) es importante que esté correctamente configurado, pues gracias a ese servicio los dispositivos de la red interna van a tener comunicación con Internet. El firewall fue configurado de tal manera que no se acepten conexiones desde Internet, al menos que se hayan solicitado desde el interior (y sólo los servicios que se han permitido).

Asimismo, actualmente se tiene funcionando la tecnología PfSense en cada uno de los planteles, en la funcionalidad de Router únicamente, el ruteo que se tiene es estático y en los casos en los que se ha integrado un nuevo plantel al nuevo esquema, se tienen que configurar las rutas estáticas.

Asimismo, se logró planear y presentar un esquema con dispositivos de red de una marca comercial. Esta red se ha implementado de manera simulada y ha presentado excelente resultados. En esa simulación se tienen varias redes LAN conectadas al equipo central, ambos conocen el protocolo de EIGRP y comparten información de enrutamiento. En esta simulación también se han integrado dispositivos en los que se supone no soportan EIGRP y se ha implantado la redistribución con éxito.

El firewall sobre OpenBSD se ha implementado con éxito, asimismo, este actualmente se utiliza transparente y con otros servicios ejecutando, como el servidor proxy, este es el encargado del filtrado de contenido, y está funcionando sin problemas.

Conclusiones generales

En el momento en el que se decidió realizar este proyecto de tesis, la propuesta que se registró con respecto al trabajo que se va a presentar, la estructura ha cambiado y desarrollado de manera confiable, esto debido a que durante la elaboración de la propuesta que se presentó aún carecía de conocimientos; sin embargo, con el avance de este tiempo, gracias a los aprendizajes adquiridos durante el proceso de creación del proyecto y aprendizaje autodidacta se alcanzaron las metas del proyecto y por tal una meta profesional más; pero también se crearon nuevas soluciones en las que se ha planteado una fecha de implementación.

La red del IEMS inicialmente antes de que arrancara este proyecto contaba con redes independientes con deficiencias, lo que originó que se planeara una restructuración de la red utilizando tecnologías libres en un inicio, como es el caso de PfSense y OpenBSD debido a que son bastante robustos y sus funcionalidades están muy bien desarrolladas y enfocadas a trabajar en redes de datos. Asimismo, su instalación y configuración es demasiado sencilla.

Se propuso una topología de red que puede ser utilizada no solo en la institución educativa, sino casi en cualquier organización que desee tener una infraestructura centralizada que brinde seguridad y servicio. Asimismo, la utilización de puertos extendidos ofrece una gran eficiencia en la comunicación entre dispositivos, pues al ser enlaces transparentes para el usuario del proveedor de servicios, el administrador de red no necesita ejecutar determinadas configuraciones para que los enlaces levanten y funcionen. Además de ello, al ser enlaces dedicados, brindan a la red privacidad, ya que los datos no son transmitidos a través de Internet.

La mejora continua de la red de datos considera la utilización de Routers de la marca Cisco, pues se analizó su funcionalidad y se determinó que sería una excelente elección montar la red sobre un diseño compuesto con esos dispositivos, porque el proveedor de los equipos es una empresa prestigiosa en la distribución de equipos de red y el soporte es que ofrecen bajo contrato es muy bueno. Asimismo, tener dispositivos de este tipo ayuda a implementar protocolos que ofrecen a la red mayor escalabilidad, funcionalidad y de rápida convergencia.

Durante el transcurso del desarrollo de este trabajo se obtuvo mucho aprendizaje, aunque no todo fue plasmado en el documento, debido a que no aplicó o porque simplemente no hubo el tiempo suficiente para su desarrollo, pero sin duda, a mi formación profesional ayudará en demasía. Así también, existieron muchos conocimientos que se adquirieron en el transcurso del desarrollo, se implementaron, funcionaron, pero fueron cambiados por otra alternativa que ofrecía mayor sencillez en su implementación.

Uno de los detalles que no se hicieron en este trabajo, pero que es muy importante, es la implementación de la redundancia de dispositivos, principalmente en los equipos que provee el proveedor de servicios (el Switch de alta velocidad) y el Router que conecta a la institución con Internet. En caso de que alguno de estos dispositivos falle, la afectación va a ser total. Por ejemplo, en el caso en el que falle la salida Internet, los planteles no tendrán acceso a la web, pero sí tendrán la capacidad de comunicarse con los demás planteles y compartir recursos y aplicaciones; sin embargo, en caso de que falle el dispositivo del proveedor de servicios, la pérdida de la conectividad será total.

En lo que respecta al trabajo colectivo, el aprendizaje también fue productivo, que, además de crear vínculos laborales, se crearon lazos de amistad y de redes de conocimientos, pues compartir y divulgar el conocimiento entre el equipo de trabajo fue fundamental para que este proyecto se concluyera.

Una de las principales dificultades que se tuvo en el proceso de este proyecto es que varias de las implementaciones que se plasman en el presente documento se realizaron de manera virtual y no de manera física, esto porque al tratarse de una organización perteneciente al gobierno, el proceso de aceptación de proyectos puede ser un gran tedio y un sinfín de historias burocráticas que impiden que los trabajos salgan a flote como se vienen desarrollando; sin embargo, actualmente la red está en la etapa en la que varios de los planteles ya se encuentran conectados a la red por medio de los puertos extendidos y utilizan un ruteo estático, debido a que se tratan de dispositivos PfSense, pero queda este trabajo como iniciativa para ir más allá.

Otra dificultad fue la organización del trabajo de equipo, eso debido a que los horarios coincidían muy poco, pero los momentos en que se logró la retroalimentación y los medios de comunicación que actualmente forman parte esencial de las relaciones humanas fueron poco a poco eliminando la problemática y convertirse en una valiosa herramienta.

Pese a los logros y problemas que se tuvieron a lo largo del proyecto, la experiencia ganada a lo largo del desarrollo de este trabajo de tesis fue importante y servirá para el futuro, tanto personal, como en la implementación de la red, en la que queda una propuesta bastante buena, a la que, sin embargo, aún se le pueden hacer varias mejoras que harían de esta red Institucional ejemplo a seguir de varias otras.

Esquema inicial de la red antes de la propuesta.

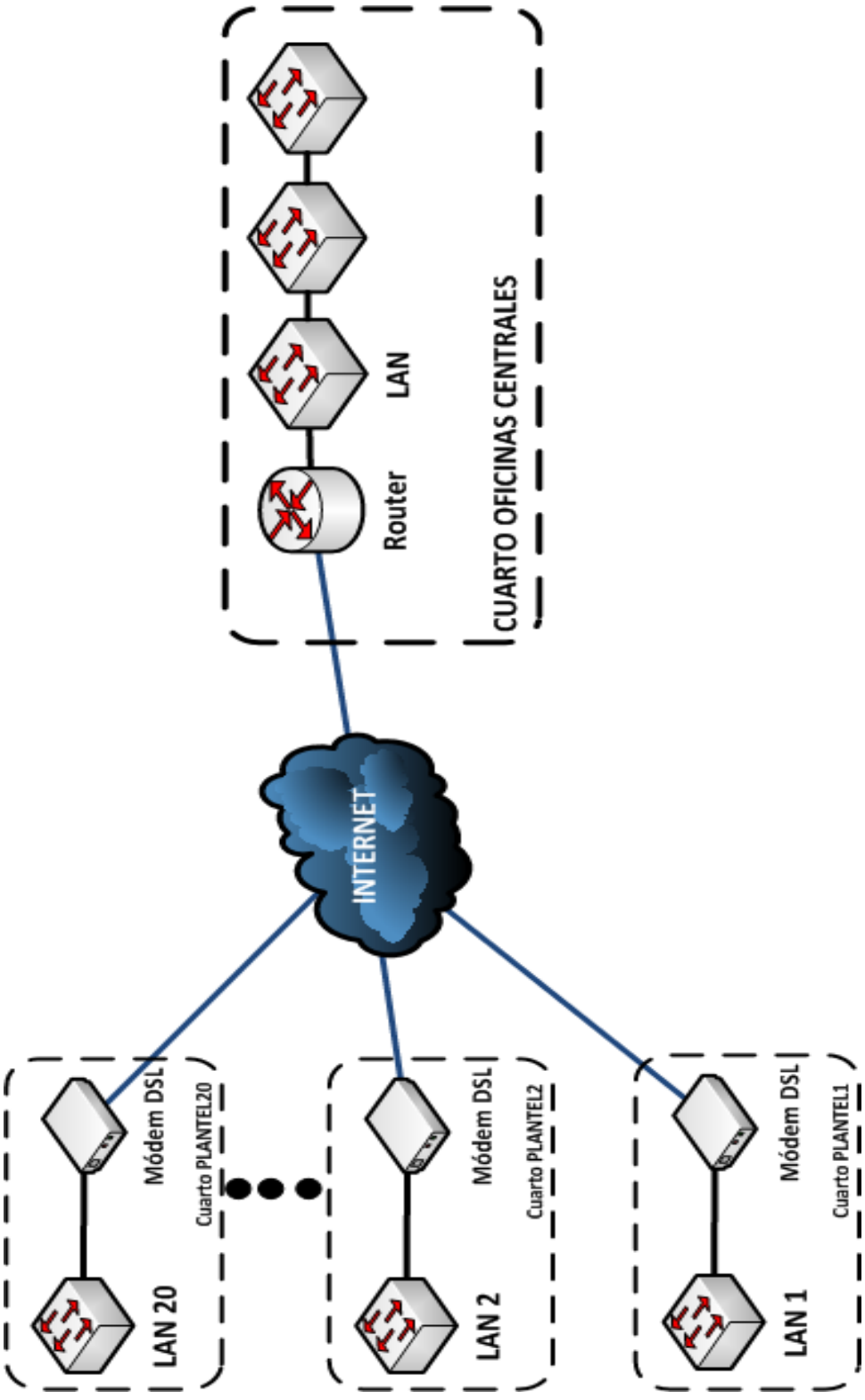

Figura 82. Esquema inicial de la red.

Esquema final resultado de la propuesta.

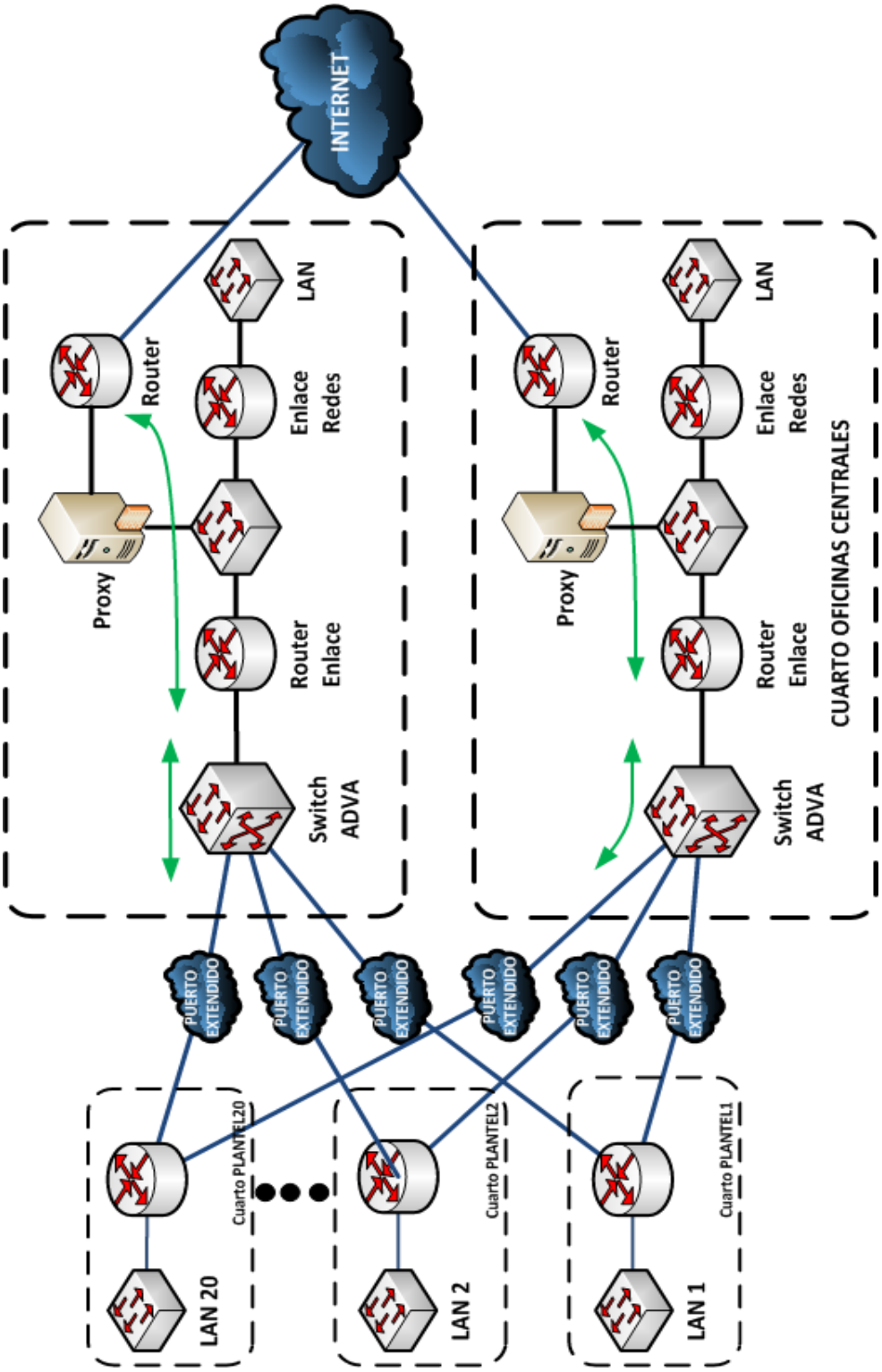

Figura 83. Esquema final de la red.

Bibliografía

[1] EC-Council. *Network Defense:Fundamentals and protocols*. Course Technology/Cengage Learning, US, 2011.

[2] Lammle, Todd. *CCNA Cisco Certified Network Associate: Fast Pass*. Sybex, US, 3rd Ed, 2008.

[3] Huntington, John. *Control Systems for Live Entertainment*. Focal Press, UK, 3rd Ed, 2007.

[4] Hesselbach, Serra, Xavie y JordiAltés Bosch. *Análisis de redes y sistemas de comunicaciones*. Edicions UPC, Barcelona, 2002.

[5] Aguilera, Purificación. *Seguridad informática*. Editex, Madrid, 2010.

[6] Robert L. Ziegler. *Linux Firewalls*. New Riders, US, 2nd Ed., 2002.

[7] Colobran, Miguel, Josep María Arqués Soldevila y Eduard Marco Galindo. *Administración de sistemas operativos de red*. Editorial UOC, Barcelona, 2008.

[8] Stanger, James, Patrick Lane&Tim Crothers. *CIW: Security Professional,Study Guide*.Sybex, US, 2002.

[9] Quezada Reyes, Cintia y Ma. Jaquelina López Barrientos. *Fundamentos de Seguridad Informática*. Facultad de Ingeniería, UNAM, 2004.

[10] López Barrientos, Ma. Jaquelina. *Criptografía*. Facultad de Ingeniería, UNAM, 2009.

[11] Buechler, Christopher M., Jim Pingle& Michael W. Lucas. *PfSense: The Definitive Guide*. Reed Media Publishing, 2009.

[12] Tanenbaum, Andrew S. and David J. *Wetherall Computer Networks*. Pearson Education, US, 5th Ed., 2011.

[13] Romero Ternero, María del Carmen, et al. *Redes Locales*. Paraninfo, Madrid, 1ra Ed., 2010.

[14] Kurose, James F. and Keith W. Ross. *Computer Networking: A Top-Down Approach*. Pearson Education, US, 6th Ed. 2013.

[15] Odom, Wendell. *CCNP Route 642-902:Official Certification Guide*. Cisco Press, USA, 2010.

[16] Segu.Info. *Firewall /Cortafuegos*. [En línea] [Citado el: 16/Jul/2011] http://www.segu-info.com.ar/firewall/firewall.htm.

[17] OpenBSD. *PF: Reservas de direcciones y balanceo de carga*. [En línea] [Citado el: 17/Jul/2011] http://www.openbsd.org/faq/pf/es/pools.html.

[18] PfSense. *PfSense*. [En línea] [Citado el: 17/Jul/2011] http://www.pfsense.org/.

[19] Boran Consulting. *Security Mechanisms*. [En línea] [Citado el: 16/Jul/2011] http://www.boran.com/security/IT1x-7.html.

[20] National Institute of Standards and Technology. *Contingency Planning Guide for Information Technology Systems*. [En línea] [Citado el: 03/Mayo/2011] http://www.itl.nist.gov/lab/bulletns/bltnjun02.htm.

[21] Cisco Systems. *Understanding the Ping and Traceroute Commands*. [En línea] [Citado el: 30 abril 2013] http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800a6057.shtml.

[22] Cisco Systems. *What is a Network Switch vs. a Router?* [En línea] [Citado el: 01/Jul/2011] http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/connect_employees_and_offices/what_is_a_network_switch/index.html.

[23] Cisco Systems. *Portable Product Sheets: Routing Performance*. [En línea] [Citado el: 01 junio 2013] http://www.cisco.com/web/partners/downloads/765/tools/quickreference/routerperformance.pdf.

[24] The Internet Engineering Task Force. *PPP over SONET/SDH*. [En línea] [Citado el: 29 mayo 2013] http://tools.ietf.org/html/rfc1619.

[25] The Internet Engineering Task Force. *Internet Protocol: Protocol Specification*. [En línea] [Citado el: 29 mayo 2013] http://tools.ietf.org/html/rfc791.

[26] The Internet Engineering Task Force. *Address Allocation for Private Internets*. [En línea] [Citado el: 29 mayo 2013] http://tools.ietf.org/html/rfc1918.

Glosario

ADSL: Asimetric Digital Subscriber Line (ADSL) es un tipo de tecnología DSL que habilita la comunicación de datos más rápido en las líneas telefónicas de cobre.

BSD: Berkeley Software Distribution (BSD, algunas veces llamado Berkeley Unix) es un sistema operativo derivado del sistema Unix nacido a partir de los aportes realizados a ese sistema por la Universidad de California en Berkeley.

CHECKSUM: Checksum o suma de hash es un dato calculado de tamaño pequeño calculado desde un bloque arbitrario de datos digitales con el propósito de detectar errores que podrían ser introducidos durante transmisión o almacenamiento.

CIDR: Classless Inter-Domain Routing (CIDR) es un método de asignación de direccionamiento IP y enrutamiento de paquetes. La IETF introdujo CIDR en 1993 para reemplazar la antigua arquitectura de diseño de redes con clase en Internet. Su objetifo fue disminuir el crecimiento de las tablas de enrutamiento y ayudar a dosificar el rápido consumo del direccionamiento IP.

Cisco Systems: Cisco Systems®: es una empresa multinacional dedicada principalmente a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

Demonio: Es un tipo especial de proceso informático no interactivo, es decir, que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario.

Dirección MAC: La dirección MAC (Media Access Control) es una dirección física y única que le asigna el fabricante a un dispositivo, tal como una tarjeta de red o un puerto. Son direcciones que cuentan con 48 bits.

FreeBSD: Sistema Operativo basado en Unix.

Full dúplex: Es un sistema que permite las comunicaciones bidireccionales, es decir, en ambos sentidos simultáneamente.

Gateway: En redes de datos, es un dispositivo (un router) que sirve como punto de acceso a otra red. Un gateway predeterminado es un nodo en la red que las aplicaciones de red usan cuando una dirección IP no coincide con otra ruta en la tabla de enrutamiento.

Hotspot: Es un sitio móvil que ofrece acceso sobre la red inalámbrica de olvidar, a pesar era por un error, se pinta.

IOS Cisco: Cisco IOS (Internetwork Operating System) es un software utilizado por varios Routers y switches del proveedor Cisco® y es un conjunto de funcionalidades de ruteo, switcheo y funciones de telecomunicaciones integrados en un sistema operativo multitarea.

Macro: Una macro enOpenBSD es una variable definida por el usuario. Estas pueden contener direcciones IP, números de puertos, nombres de interfaces, etc. Son utilizadas para reducir la complejidad del grupo de reglas del filtro de paquetes, así como para facilitar el mantenimiento de las mismas.

Malware: Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.

Memoria caché: La memoria caché es una clase de memoria RAM estática (SRAM) de acceso aleatorio y alta velocidad, situada entre el CPU y la RAM; se presenta de forma temporal y automática para el usuario, que proporciona acceso rápido a los datos de uso más frecuente.

Métrica: Método por el cual el algoritmo determina que ruta es mejor que otra. Esta información se guarda en las tablas de enrutamiento.

Paquete: agrupación lógica de información que incluye un encabezado que contiene información de control y datos del usuario. Se utilizan para referirse a las unidades de datos utilizadas en la capa de red del modelo OSI.

PING: (Packet InterNet Groper) es una utilidad que se usa para verificar que un paquete de datos se pueda distribuir a una dirección sin errores. El comando ping es un método comúnmente utilizado para la resolución de problemas de accesibilidad a la red de dispositivos. Este comando envía mensajes eco por medio del protocolo de control de mensajes de internet (ICMP) para determinar si el host remoto está activado o desactivado, determinar el retardo de la comunicación entre los host, así como la pérdida de paquetes.

PPP: El Protocolo Punto a Punto es el encargado de suministrar conexiones de Router a Router y de host a red por medio de circuitos síncronos y asíncronos.

Puerto: Un puerto es un mecanismo que se utiliza para identificar un determinado servicio o proceso en una computadora. Un ejemplo es el puerto 80 en un servidor web, es ahí donde él recibe peticiones de acceso al servicio por parte de los clientes.

SDH: Un estándar internacional para redes ópticas de telecomunicaciones de alta capacidad. Un sistema de transporte digital sincrónico diseñado para proveer una infraestructura más sencilla, económica y flexible para redes de telecomunicaciones.

Sistema autónomo: Un Sistema Autónomo (AS) es un conjunto de redes con una administración común que comparten una estrategia de enrutamiento común.

SONET: Estándar que permite las comunicaciones con transmisión de paquetes en forma de protocolo punto a punto

SSH: (Secure Shell, Shell Segura) es el nombre de un protocolo, pero también de un servicio que brinda comunicación entre equipor remotos a través de una sesión cifrada.

Subinterfaz: Una subinterfaz es la división de una interfaz física en una o más interfaces virtuales.

Tabla de enrutamiento: La tabla de enrutamiento se almacena en memoria de un Router o en otro dispositivo conectado a la red. Esta guarda un registro de las rutas a destinos particulares en la red.

TACACS: TACACS (Terminal Access Controller Access-Control System) es un protocolo de autenticación comúnmente utilizado en redes UNIX que permite la autenticación remota a un servidor o dispositivo enviando usuarios y contraseña a un servidor de autenticación que determina si es permitido el acceso a dicho sistema. Este protocolo es capaz de ofrecer perfiles de usuario por autenticación y autorización .

Telnet: Telnet (TELecommunication NETwork) es el nombre de un protocolo de red y aplicación que permite la comunicación con dispositivos remotos a través de un canal sin cifrar.

Trama: La PDU (Protocol Data Unit, Unidad de Datos de Protocolo en español) de la capa 2 que ha sido codificada por un protocolo de la capa de enlace para su transmisión digital.

URL: Un Localizador de Recursos Uniforme, más comúnmente denominado URL (sigla en inglés de Uniform Resource Locator), es una secuencia de caracteres, de acuerdo a un formato modélico y estándar, que se usa para nombrar recursos en Internet para su localización o identificación.

VPN: Las Redes Privadas Virtuales son una manera de conectar una LAN privada a un sitio remoto como Internet o cualquier otra red insegura transportando datos privadamente usando cifrado.

NetBSD: NetBSD es un sistema operativo de la familia Unix, de código abierto y libre. Un puerto es un mecanismo que se utiliza para identificar un determinado servicio o proceso en una computadora. Un ejemplo es el puerto 80 en un servidor web, es ahí donde él recibe peticiones de acceso al servicio por parte de los clientes.