FACULTAD DE EDUCACIÓN TECNICA PARA EL DESARROLLO

CARRERA DE INGENERÍA EN TELECOMUNICACIONES

TEMA:

"Diseño e implementación de un laboratorio para prácticas de configuración y operación de redes con utilización de protocolos de enrutamiento"

Previo a la obtención del título

INGENIERO EN TELECOMUNICACIONES CON

MENCIÓN EN GESTIÓN EMPRESARIAL EN TELECOMUNICACIONES

Elaborado por:

Jury Cristóbal Figueroa Flores

Jorge Emilio Aguiar Matías

Guayaquil, septiembre 2013

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

CERTIFICACION

Certifico que el presente fue realizado en su totalidad por los Sres. Jorge Emilio Aguiar Matías y Jury Cristobal Figueroa Flores como requerimiento parcial para la obtención del título de INGENIERO EN TELECOMUNICACIONES CON MENCION EN GESTION EMPRESARIAL EN TELECOMUNICACIONES.

Guayaquil, Septiembre del 2013

INGENIERO CARLOS ZAMBRANO MONTES
DIRECTOR

INGENIERO NESTOR ZAMORA

INGENIERA LUZMILA RUILOVA

REVISADO POR :

INGENIERO ARMANDO HERAS

RESPONSABLE ACADÉMICO

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

DECLARACION DE RESPONSABILIDAD

JURY CRISTOBAL FIGUEROA FLORES

JORGE EMILIO AGUIAR MATIAS

DECLARAMOS QUE:

La tesis de grado denominada "**Diseño e implementación de un laboratorio para prácticas de configuración y operación de protocolos de enrutamiento".** Ha sido desarrollada en base a varias guías de networking, en su mayoría extraída del manual de CCNA exploration 2 pero solo como guía de conocimiento mas no su entera literatura, debido a que los protocolos son conjuntos de reglas establecidas por tanto su modificación no es motivo del estudio de esta publicación, pero su explicación es totalmente autoría de los antes mencionados y por tanto responsabilidad de los autores.

En virtud de esta declaración, nos responsabilizamos del contenido, la veracidad y el alcance científico que se le dé a esta tesis de grado.

Guayaquil, Septiembre del 2013

LOS AUTORES:

JURY CRISTOBAL FIGUEROA FLORES

JORGE EMILIO AGUIAR MATIAS

Universidad Católica Santiago de Guayaquil
Facultad de Educación Técnica para el Desarrollo

Carrera de Ingeniería en Telecomunicación

AUTORIZACION

NOSOTROS:

JORGE EMILIO AGUIAR MATIAS

JURY CRISTOBAL FIGUEROA FLORES

Autorizamos a la Universidad Católica de Santiago de Guayaquil, la publicación en la biblioteca de la institución de la tesis de grado "**Diseño e implementación de un laboratorio para prácticas de configuración y operación de protocolos de enrutamiento".** Cuyo contenido, ideas y criterios son de nuestra autoría.

Guayaquil, Septiembre del 2013

LOS AUTORES:

JURY CRISTOBAL FIGUEROA FLORES

JORGE EMILIO AGUIAR MATIAS

AGRADECIMIENTO

Dedico este trabajo a Dios y a mis Padres Jury Atilio Figueroa Loor y a Lilian Fantina Flores Castillo quienes además de ser dadores de vida, siempre estuvieron pendientes de mí, apoyándome. Agradezco a mi tía la Ing. Aura Figueroa por haberme siempre servido de ejemplo y por su consejo y capacidad de incitarme a hacer las cosas bien, a mi tío Cristóbal Figueroa Loor a quien siempre he llamado mi segundo papá, quien siempre estuvo pendiente de mi desempeño tanto personal como académico, a mi Tía Lic. Janeth Figueroa quien siempre estuvo preocupada por mi salud , a mi tía Angelita quien a la distancia siempre supo darme su apoyo, a toda mi familia en general quienes cuando fue necesario supieron darme la llamada patadita de confianza para poder seguir adelante. A mi compañero de Tesis Jorge Aguiar quien además de mi compañero de tesis siempre fue mi mejor amigo, a su mamá la Sra. Soraya de Aguiar quien me abrió las puertas de su domicilio no solo mientras era solo un estudiante sino durante el desarrollo de esta tesis.

Agradezco a la Universidad Católica Santiago de Guayaquil por abrirme sus puertas para mi educación superior, Al decano de la Facultad Técnica para el desarrollo Ing. Manuel Romero , al Director de Carrera Ing. Armando Heras y al Ing. Luis Córdoba por su paciencia y guía para el desarrollo e ingreso de esta publicación.

Agradezco al Ing. Carlos Zambrano y al Ing. Néstor Zamora por prestarme todo su apoyo durante el desarrollo de este trabajo, al Ing. Galo Cornejo mi profesor de Cisco por impartirme todo su conocimiento para el desarrollo y mejor explicación de todos y cada uno de los protocolos mostrados en esta publicación.

A la Ing. Yajaira Vergara por la prestación de facilidades para el desarrollo de esta tesis

A mi prima Karla Maldonado por siempre estar ahí pendiente de mí quien en un momento de deserción supo ayudarme a buscar la mejor solución para no tomar esa actitud.

Agradezco finalmente a todos los catedráticos de la Carrera de Ingeniería en Telecomunicaciones por saber formar profesionales de calidad y por inducirnos al pensamiento crítico y deductivo, y por saber cultivar la inteligencia que tenemos nosotros como estudiantes para así lograr lo mejor de nosotros mismos.

A todos gracias.

Atte.:

Jury Figueroa Flores.

AGRADECIMIENTO

Ante todo deseo dedicar a Dios el fruto no solo este trabajo, sino las bendiciones brindadas durante el desarrollo de esta etapa, en el cual me he visto formado con valores fundamentales para aplicar en el reto de la vida profesional. A mi madre Sra. Gladys Soraya Matías Yépez y mi padre Eco. Emilio Aguiar Verdesoto que sembraron desde muy pequeño en mí el valor y los principios para afrontar las diferentes circunstancias, a enseñarme a ver que un resbalón no es un fracaso, sino que aprovechar la caída para tomar impulso y alcanzar mis ideales. Una especial mención a la Sra. Gladys Yépez Antón que con consejos siempre me dio la mano y complementando con el cariño de una abuela ha inculcado buenos sentimientos, a valorar el día a día y aprovechar al máximo toda oportunidad brindada sin perder la sencillez de la cual ella es un digno ejemplo.

Me gustaría nombrar a cada miembro de la familia que supieron orientarme, cada uno con una cualidad diferente del cual se puede enaltecer la unión que han mantenido de manera ejemplar, siendo todos unos pilares fundamentales reflejados en la familia y decisiones tomadas.

A mi amigo fraterno Jury Figueroa Flores que me ha demostrado una amistad sincera y apoyo incondicional, complementando este trayecto estudiantil con las ocurrencias propias de la juventud, responsabilidad y la acogida cálida de su familia. De igual manera a todos mis amigos que fui conociendo a lo largo de esta carrera, haciendo una placentera convivencia cada día transcurrido en la universidad.

Agradezco a los profesores que nos colmaron de conocimientos, convirtiéndose en unos verdaderos guías, aclarando y desarrollando en nosotros personas capaces para afrontar este campo tan competitivo.

Finalmente mi más sincero agradecimiento a la Universidad Católica Santiago de Guayaquil que con los valores que tanto apostaron en nosotros, han creado en toda su vida académica profesionales muy competitivos tanto en el ámbito profesional como en lo personal.

Para todos muchas gracias y bendiciones.

Atte.:

Jorge Emilio Aguiar Matías.

Índice:

Indice de Figuras

Resumen

En la actualidad las redes son parte de nuestra vida todos o la gran mayoría de los aparatos que se usan actualmente están conectados o son parte de una red ya sean estas redes mediante las cuales se puede tener voz , datos , video.

Estas redes tienen en la actualidad exigencias por tráfico, las cuales son cada vez mayores. Es el trabajo del Ingeniero en Telecomunicaciones la instalación y el mantenimiento de las mismas ya sean estas redes cableadas o inalámbricas. Es por esta razón que es necesario que el Ingeniero en telecomunicaciones este entrenado para poder instalar y solucionar problemas que se den con las mismas.

La malla curricular actual de la Universidad católica Santiago de Guayaquil para la carrera de ingeniería en Telecomunicaciones carece en la actualidad de materias que nos enseñen el funcionamiento práctico de los protocolos de enrutamiento, los cuales son la base actual de las redes. Estos conocimientos deben ser adquiridos por el alumnado en institutos que funcionan muy aparte de la Facultad Técnica para el Desarrollo. Estos cursos no solo son caros, sino que también son motivo de uso de tiempo que el alumnado de la Facultad Técnica para el Desarrollo, tiempo, que en su mayoría no tienen.

Esta Tesis centra su estudio en el funcionamiento y configuración de los protocolos de enrutamiento mas utilizados en la actualidad en la mayoría de redes corporativas que funcionan no solo en Ecuador sino a nivel mundial. Lo cual se volveria una

ventaja para todos los estudiantes, ya que, estos protocolos se verían como parte de las materias que los imparten teóricamente y no como cursos después de la carrera.

Como parte de esta Tesis se entrega un manual de prácticas de laboratorio las cuales tienen sus respectivas topologías simuladas en el programa de simulación llamado Packet Tracer y un conjunto de tareas las cuales ayudaran al alumnado a comprender mejor el funcionamiento de los protocolos de enrutamiento dinámico; Se entregan también dos routers de alto tráfico marca CISCO modelo 1841 con el cableado necesario para poder armar estas prácticas de laboratorio en capa física, de esta manera el alumnado de la Facultad Técnica para el desarrollo experimentará posibles fallas que se puedan dar durante una configuración en caliente.

El uso de la marca CISCO como modelo de router y como respaldo de plataforma es debido a las otras marcas de equipos se basan en tecnología CISCO haciendo uso o pequeñas varianzas en la implementación de los protocolos de enrutamiento pero los protocolos de enrutamiento no cambian, siguen siendo bases de CISCO.

Es necesario que el Ingeniero en Telecomunicaciones de hoy y del futuro tenga esta capacitación pues el mercado laboral lo requiere, esto pondría al Ingeniero en telecomunicaciones graduado en la Facultad Técnica para el Desarrollo como primera opción al momento de que los patronos elijan a la persona que trabaja con ellos.

Capítulo 1:

1 Generalidades

En este capítulo se presentan las generalidades de este proyecto, una introducción a la problemática que este proyecto pretende solucionar y sus objetivos de elaboración para llegar a una meta común.

1.1 Introducción

Las nuevas tecnologías de la información y la comunicación se basan en redes inteligentes que evolucionan constantemente, es decir cada día crecen más es responsabilidad del Ingeniero en Telecomunicaciones el mantenimiento y reparación de estas pero para esto el ingeniero debe estar formado para poder hacer lo antes mencionado para esto se necesita tener conocimiento de los protocolos de enrutamiento que son la base de la entrega de paquetes dentro de una red.

El enrutamiento es el corazón del networking sin él la red se volvería un caos total es por esta razón que el router va a ser la base inteligente de la red, pues este es el que se encarga de manejar el tráfico de la red y de llevar o enrutar el paquete a cada uno de los puntos de la red.

Existen varios tipos de enrutamiento, el enrutamiento estático y el enrutamiento dinámico, ambos motivo de estudio de esta publicación. El enrutamiento estático es usado en redes pequeñas y su uso es muy limitado pues se vuelve tedioso al momento de la configuración mientras el dinámico hace su configuración mucho más rápida y sencilla, pero para su configuración es necesario que se tenga conocimiento

del funcionamiento de este pues al momento de su funcionamiento se podrían dar problemas.

Durante el desarrollo de esta publicación se va a ir demostrando de a poco el funcionamiento y la configuración de los protocolos de enrutamiento estático y dinámico

1.2 Contextualización del Tema

Las herramientas de networking son utilizadas en la vida cotidiana de toda persona que trabaja ante un computador personal conectada a diversos sistemas de comunicación (Intranet, Internet, redes privadas como redes públicas), lo que intentamos demostrar mediante la implementación de un laboratorio de prácticas de protocolos de enrutamiento es que se puede formar ingenieros que el mercado laboral requiere, lo que nos permitirá como Facultad Técnica para el Desarrollo de la Universidad Católica de Santiago de Guayaquil dar el primer paso a orientar nuestra malla curricular al networking.

1.3 Planteamiento y delimitación del tema

Todo ingeniero en Telecomunicaciones debe de tener conocimientos sólidos de estructura básica de redes, la cual se adquiere mediante la práctica tanto en configuración como en interacción física con los equipos, el marco teórico que lo soporte debe ser parte del programa y Syllabus de una nueva materia de Conmutación telefónica II, orientada a las asimilación de competencias en redes convergentes basadas en IP, cuyo conocimiento práctico se lo realizara en las

practicas definidas en el presente trabajo de titulación; por lo que el propósito de este proyecto es implementar un laboratorio de Networking, para poder hacer prácticas directamente con los equipos a ser implementados como Puentes, Hub, Switches, Ruteadores, etc.**,** además de hacer uso del software simulador packet tracert que estará incluido en el laboratorio a implementarse, lo que permitirá prácticas previas a la configuración de los equipos, con las diferencias naturales de configuración por las variantes según el modelo del equipo.

1.4 Justificación

La Facultad Técnica del Desarrollo debe orientar su malla curricular a las tendencias de la industria de las Telecomunicaciones, esto es el networking, el profesional graduado debe haber adquirido las competencias exigidas por el mercado en las pruebas de destreza laboral, las empresas buscan ingenieros en telecomunicaciones con conocimientos sólidos en sistemas de tecnologías convergentes basados en redes multiservicios que utilizan los protocolos de última generación, en hardware con sistemas propietarios que a pesar que utilizan protocolos estandarizados, lideran la provisión de infraestructura en el mercado, así como globalmente han posicionado un sistema de capacitación y certificación exigida actualmente en el 100% de los perfiles de requerimientos de Talento Humano en lo que a reclutamiento de Ingenieros en telecomunicaciones se refiere. **(Ver Figura 1)** y comparar con **Figura** 2 **(Ver Figura 2)**

El propósito del presente trabajo de titulación es proporcionar a los alumnos de ingeniería en telecomunicaciones, el tener el acceso y la oportunidad de aprender

mediante prácticas de laboratorio acerca del funcionamiento e implementación de protocolos de enrutamiento y su aplicación; que aporten al estudiante de Ingeniería de Telecomunicaciones, la adquisición de las destrezas exigidas por el mercado.

1.5 Objetivos

Los objetivos planteados en esta publicación son los siguientes:

1.5.1 Objetivo General

- Desarrollar el conocimiento y las destrezas en el ingeniero en telecomunicaciones graduado en la Facultad Técnica de la Universidad Católica Santiago de Guayaquil, para cumplir eficiente y eficazmente con su rol ante los requerimientos de la sociedad y el mercado Implementando un laboratorio de Networking para prácticas de conceptos y protocolos de enrutamiento, dotando a el laboratorio de equipos para la implementación de dichas prácticas.

1.5.2 Objetivos Específicos

- Analizar las características de los equipos brindados para la implementación de protocolos
- Implementar y configurar la infraestructura necesaria al laboratorio para la implementación de las prácticas.
- Desarrollar y configurar prácticas base para la operación de cada uno de los protocolos de enrutamiento que enmarcan en el estudio de esta publicación.

Capítulo 2

2 Conocimientos básicos de networking

2.1 Introducción al capitulo

En la actualidad hacemos mucho uso de las redes en nuestras vidas pues utilizamos sus aplicaciones a diario ya sea haciendo uso de la internet o voz sobre IP[1] o las aplicaciones de las redes sociales que son las más usadas en estos días o ya sea las soluciones empresariales como intranet o compartición de archivos dentro de una LAN[2] las cuales facilitan nuestras vidas.

El centro de una red es el Router, pues el router es el encargado de compartir paquetes entre redes es decir conecta una red con otra red. Un router maneja varios tipos de paquetes en los cuales se tratan según capa 3 del modelo OSI[3] (Open System Interconnection) o Red generalmente paquetes IP, el destino de estos paquetes puede ser un servidor web al otro lado del mundo o un servidor POP3[4] de correos a tres cuadras de donde se origina un paquete. La eficiencia de un paquete al enviarse a través de una internetwork depende en su mayoría de la capacidad de un router en enviar estos paquetes de la mejor manera posible de tal manera que el paquete no demore mucho en llegar y no se pierda en el proceso.

Aseguran la conectividad 24 horas del día los 7 días a la semana y la garantizan pues en caso de alguna ruptura de algún enlace utilizan rutas alternas para entregar un paquete.

---

[1] Protocolo de comunicación de datos digitales, “Internet Protocol”.
[2] "Local Area Network", red de pequeña área.
[3] "Open Systems Interconnection", Norma universal para protocolos de comunicación lanzado en 1984.
[4] "Post Office Protocol", Protocolo de recepción para gestionar correo electrónico a través de la red.

Proveen nuevos servicios integrados de datos, voz y videos ya sea por cable o sin él, es decir inalámbricas, los routers dan prioridades a los paquetes IP según el QoS[5] o calidad de servicio lo cual asegura la continuidad de paquetes que se entregan en tiempo real llámese así a la voz pues es necesario mantener ciertos estándares el rato de la transmisión.

Todos estos servicios son servicios que pueden ser brindados por un router y su responsabilidad es enviar los paquetes a la red siguiente. La conductividad y convergencia[6] de una red solo se logra gracias a la capacidad de enrutar paquetes entre ellas.

2.2 Dentro del router

Un router es como un computador solo que este computador está diseñado para enrutamiento de paquetes. El primer ruteador fue utilizado para la red que fue el origen de internet, la red de la (ARPANET), fue con un procesador (IMP). El IMP era un procesador de un computador Honeywell 316, la cual fue la que le dio origen a ARPANET el 30 de agosto de 1969.

Muchos routers tienen los mismos componentes de una computadora normal

CPU[7]

RAM [8]

[5] "Quality of Service", tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo determinado.
[6] Capacidad de diferentes plataformas de red para transportar servicios o señales similares.
[7] "Central Processing Unit", unidad central de procesamiento.

ROM[9]

Sistema Operativo

Los routers siempre determinan la mejor ruta para llegar de una red a otra, pues se podría decir que su principal tarea es dirigir los paquetes entre redes locales y remotas.

El router usa su tabla de enrutamiento para determinar la mejor ruta para redistribuir el paquete haciendo una evaluación de lo que se llamaría como métrica distancia cantidad de saltos donde el router hace una serie de cálculos para hacer su trabajo "determinar la mejor ruta". Cuando un router recibe un paquete de capa 3 IP, lo toma, lo des encapsula, verifica la dirección IP de destino y lo revisa en su tabla de enrutamiento, si la dirección se encuentra dentro de su tabla de enrutamiento lo toma y lo reenvía hacia el dispositivo final al cual se encuentra destinado el paquete, caso contrario verifica dentro de la tabla de rutas generales la mejor vía para enviar el paquete a la red que debería de recibirlo.

Es bastante probable que dentro de la transmisión de paquetes el router reciba un paquete con un encapsulado de una trama de enlace de datos , como por ejemplo podría ser una trama Ethernet , y al enviar un paquete, el router enviará

[8] "Random-Access Memory", memoria desde donde el procesador recibe las instrucciones y guarda los resultados.

[9] "Read-Only Memory", memoria que se utiliza para almacenar los programas que ponen en marcha el ordenador.

este con otro tipo de trama de enlace de datos como por ejemplo una PPP[10]. Esta encapsulación depende del tipo de interfaz por la que salga el paquete además también por el tipo de medio al que se conecta esto puede incluir tecnologías LAN , como Ethernet y conexiones seriales como interfaces WAN[11] , además de esto la conexión T1[12] que utiliza PPP , frame relay[13] y modos de transferencia asíncrona (ATM[14]).

2.2.1 Memorias y CPU del router

Existen varios tipos y modelos de router. Todos tienen componentes de hardware distintos. La ubicación de dichos componentes varía según el modelo del router, dentro de las figuras del capítulo se encuentran figuras del interior de un router cisco 1841 que es el modelo de router que se entrega adjunto con el proyecto de titulación o tesis al que nos referimos en este momento. Para observar un router en sus interiores es completamente necesario remover la cubierta metálica que viene en el mismo para lo cual necesitaremos un destornillador. Generalmente esto no es necesario hacerlo pues una vez abierto el router pierde su garantía por eso no recomendamos que se abran los equipos que se entregan. **(Ver Figura 1)**

[10] "Point-to-Point Protocol", Protocolo que permite establecer una comunicación a nivel de enlace entre dos ordenadores.
[11] "Wide Area Network", redes informáticas que se extienden sobre un área geográfica extensa o conjuntos de LANs.
[12] Servicio de acceso a Internet que provee una transferencia de datos de hasta 1.5 Mbps.
[13] Técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual.
[14] "Asynchronous Transfer Mode", protocolo de comunicaciones definido para comunicaciones de datos a alta velocidad.

Al igual que una PC un router tiene ciertos componentes, trataremos de hacer una breve descripción de cada uno de ellos e indicaremos su uso dentro del router.

CPU.- El CPU al igual que en una pc ejecuta las instrucciones que genera el sistema operativo entre las cuales esta: el inicio del sistema, funciones de conmutación y enrutamiento.

RAM.- La RAM (Random Access Memory) almacena las instrucciones y los datos necesarios que la CPU debe de ejecutar. Dentro de las instrucciones se pueden almacenar los siguientes componentes:

- El sistema operativo Cisco IOS este se copia en la RAM durante el inicio también llamado startup config.
- Archivo de configuración en ejecución también llamado running config
- Tabla de enrutamiento IP
- Cache ARP. Esta contiene la dirección IPv4 para la asignación de direcciones MAC[15], este proceso es similar a las a la cache ARP de una PC. Esta se usa en routers que tienen interfaces Ethernet de LAN.
- Búfer de paquete los paquetes se almacenan temporalmente en el búfer cuando se reciben por una interfaz o son enviados a través de una, pues se hace una fragmentación para enviarlo por partes hasta que se recibe el paquete completo.

[15] "Media Access Control", dirección de hardware única que identifica a cada nodo de una red.

Cabe recalcar que la RAM es una memoria volátil y se pierde al momento de mandar a reiniciar el router.

ROM.- la ROM (Read Only Memory) es una manera de almacenamiento permanente generalmente los dispositivos de Cisco que manejan sistema Operativo Cisco IOS guardan en la ROM los siguientes ítems.

- Instrucciones de bootstrap
- Software básico de diagnostico
- Versión de Cisco IOS más básica

Cabe recalcar que la ROM no pierde su información el rato de apagar el router.

Memoria flash.- la memora flash es una memoria que se puede borrar y reescribir eléctricamente cabe recalcar que no es una memoria volátil, esta se utiliza como memoria permanente del sistema operativo Cisco IOS , este para los procesos se copia en la RAM de donde entonces es utilizado por el procesador del router.

Nvram.- (No volátiles RAM) como su nombre lo dice es una RAM no volátil es decir no pierde su información cuando se desconecta el router. El Cisco IOS utiliza esta parte de la memoria Nvram para guardar ciertos archivos de configuración como el startup-config que es la configuración del inicio del router esta será cambiada en cada configuración que se haga dentro del running config mediante el comando copy running-config to startup-config

.

2.2.2.- Proceso de arranque del router

Este proceso sigue los siguientes pasos:

1. Ejecución de la POST.
2. Carga de la Bootstrap
3. Ubicación y carga del software IOS de cisco
4. Ubicación y carga de configuración de inicio o ingreso al modo setup.

Ejecución del POST.- (power on self test) es un proceso común que sufre cualquier pc el rato de iniciarse, como nuestro router es igual que cualquier pc también lo sufre dentro de este test se prueba el funcionamiento de cada una de las interfaces y memorias del router.

Carga del bootstrap.- después de que se ejecuta el POST se ejecuta la copia del programa bootstrap donde se hace una copia de la ROM a la RAM del router. El procesador ejecuta las instrucciones el programa bootstrap cuya función principal es encontrar el boot del IOS de cisco y subir este en la RAM.

Ubicación y carga del software IOS de cisco.- Se encuentra el ios y comienza la ejecución del mismo, este generalmente se almacena en el flash, pero también puede almacenarse en un servidor TFTP[16]. En caso de que no se encuentre una imagen

[16] "Trivial file transfer Protocol", protocolo de transferencia muy simple semejante a una versión básica de FTP.

completa del IOS. Se hace una copia de una versión más básica del IOS en la RAM. Esto ayudará para diagnosticar cualquier problema y esto puede usarse para cargar una versión completa en la RAM.

Ubicación y carga del archivo de configuración.- se busca el archivo de configuración de inicio. Una vez que se carga el IOS, el bootstrap busca en la NVRAM el archivo de configuración inicial comúnmente conocido como startup-config y automáticamente se hace una copia del mismo en la RAM llamándose a este running-config. El startup-config tiene en su configuración:

- Direcciones de cada una de las interfaz
- Información de enrutamiento
- Contraseñas
- Cualquier otra configuración guardada por el administrador de red

Ingreso al modo setup.- este modo es un modo opcional es como un install wizard donde se da configuración inicial al router. En este modo no se puede realizar configuración avanzada es por eso que los administradores de red casi no utilizan este modo.

Cuando se inicia el router por primera vez sin tener configuración alterada, el router arroja el mensaje:

> Would you like to enter the initial configuration dialog? [yes/no]: no (Systems, 2012)

El modo setup se iniciara cuando se responda con un yes en la pregunta.

Interfaz de línea de comandos.- cuando se responde que no al modo setup va a aparecer el siguiente mensaje:

> Would you like to terminate autoinstall? [Yes]: <Enter>
>
> Press the Enter key to accept the default answer.
>
> Router>
>
> (Systems, 2012)

Este es la interfaz de línea de comandos.

2.3 Interfaces del router

2.3.1 Puertos de administración

Los puertos de administración son puertos mediante los cuales se pueden hacer cabios a la configuración inicial del router. El puerto más común en los puertos de administración es el puerto de consola, el cual efectivamente como se mencionó anteriormente sirve para conectar el router a un terminal o también llamada PC

dentro de este mediante una conexión serial controlada y sincronizada permite accesar a la configuración del router haciendo cambios en el flash y la RAM.

Otro puerto de administración aunque poco común y muy poco utilizado es el puerto auxiliar, a pesar de que no todos los routers los traen es un puerto bastante útil cuando se desea configurar y no se tiene un cable de consola.

El termino interfaces en los routers cisco se refiere a los puertos físicos del router de los cuales se puede sacar información dentro de las cuales tenemos los puertos administrativos explicados anteriormente y las famosas interfaces WAN y LAN las cuales manejaremos en toda la explicación de esta tesis.

Interfaces LAN.

Las interfaces LAN son como su nombre lo dice interfaces que están dedicadas a aplicaciones dentro de una red local LAN (local area network) estas pueden ser: puertos Ethernet, Giga Ethernet, coaxiales, entre otros.

Interfaces WAN.

Las interfaces WAN son como su nombre lo dice interfaces dedicadas a soluciones WAN (wide area network) que generalmente comunican dispositivos intermedios

con dispositivos intermedios. Estos pueden ser puertos seriales, puertos ISDN[17] o en, y lo que es frame relay, puertos ópticos para redes FTTH[18] entre otros.

Routers trabajando en capa de red

El trabajo de un router en si como su nombre lo indica es conectar múltiples redes es por eso que anteriormente hemos llamado a este dispositivo un dispositivo interredes, es por eso que se considera a este dispositivo como un dispositivo de capa 3 esto haciendo referencia al modelo OSI el cual veremos un poco más explicado más adelante, la capa 3 del modelo OSI es la capa de red. Donde específicamente se busca la mejor ruta entre dos o más IP para entregar un paquete.

Cuando a un router le es entregado un paquete, este examina su IP de destino. Si la dirección de destino no se encuentra dentro de las redes y subredes administradas por el router, el mismo reenvía el paquete al siguiente router en la red.

2.4 Enrutamiento de Paquetes

Cuando se está trabajando con una red preestablecida o se diseña una red nueva se necesita siempre tener en claro que es necesario documentar esta red, es decir, se

[17] "Integrated Services Digital Network", Protocolos de comunicación para permitir redes telefónicas transportar datos, voz, y otro tipo de material.
[18] "Fiber To The Home", utilización de cables de fibra óptica y sistemas de distribución ópticos adaptados a esta tecnología para la distribución de servicios avanzados.

debe de poner en esta documentación entre otras cosas un diagrama que indique la topología que esta red debe de tener además de una tabla de direccionamiento que incluya lo siguiente

- Nombres de los equipos o dispositivos que se van a manejar en la red
- Interfaces que van a ser usadas para la conexión con cada uno de ellos
- Direcciones IP y máscaras de subred, además de las direcciones de Gateway asignadas a cada uno de ellos
- Carga de la tabla de direcciones

2.5 Configuración Básica de un router Cisco

En este ítem se manejaran los siguientes puntos

- Asignar un nombre al router
- Configuración de contraseñas
- Configuración de cada una de las interfaces
- Configurar un mensaje de bienvenida
- Guardar cambios en el router
- Verificar la configuración básica

En un router cisco existen varios modos la primera petición se encuentra en modo usuario el cual deja ver el estado del router pero no permite modificar absolutamente nada de la configuración el estado del modo usuario es el siguiente:

Router>

(Systems, 2012)

El comando “enable” nos va a permitir ingresar al modo EXEC privilegiado. Este modo nos va a permitir ingresar la configuración del router y realizar cambios se verá de la siguiente manera:

Router>enable

Router#

(Systems, 2012)

Como se puede ver se cambia de estado indicando el signo # lo cual indica que se está en modo exec privilegiado.

Asignación de un nombre al router

Para asignar a un nombre al router hay que realizar los pasos antes mencionados e ingresar además al modo de configuración global, esto se hará mediante el uso del comando “configure terminal” de esta manera se ingresara al modo como se muestra a continuación:

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#

(Systems, 2012)

Nos podemos dar cuenta que estamos en el modo de configuración global porque tenemos (config) # en la última sentencia.

Para asignar un nombre al router se podrá hacer uso del comando “hostname” donde se hará esto de la siguiente manera: Hostname nombre, donde nombre va a ser el nombre valga la redundancia que se quiere poner al router. Se podrá hacer de la siguiente manera:

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname Jury

Jury(config)#

(Systems, 2012)

Como podemos ver al final nos cambia el nombre de router a Jury que es el nombre que utilizamos para poder identificar al router.

Configuración de contraseñas del router

Ahora para configurar las seguridades protegidas por contraseñas del router se puede utilizar el comando “enable password” el cual habilitara una contraseña la cual **no**

será encriptado, pero la explicaremos porque será importante su uso en factores posteriores. Se hará de la siguiente manera: Enable password clave donde la contraseña será la palabra clave, esto habilitara el uso de contraseña para la entrada al modo de privilegiado. Se mostrará de la siguiente manera

Jury(config)#enable password clave

(Systems, 2012)

De esta manera cuando se ingrese al dispositivo se pedirá la contraseña y nos saldrá lo siguiente:

Jury>enable

Password:

Password:

Jury#

(Systems, 2012)

Pero la gran debilidad de este comando es que las contraseñas no son encriptados es decir no se las esconde de esta manera somos sensibles a cualquier ataque dentro de la red pues cualquier persona puede ingresar a este modo y hacer cambios en la configuración, al hacer un show running-config que se puede hacer desde modo usuario podremos ver la clave de nuestro router sin encriptarse. Esto lo podemos ver de la siguiente manera:

Jury#sh run

Building configuration...

Current configuration: 472 bytes

!

Version 12.4

No service timestamps log datetime msec

No service timestamps debug datetime msec

No service password-encryption

!

Hostname Jury

!

!

!

Enable password clave

(Systems, 2012)

Como podemos ver en lo que resulta del comando ingresado anteriormente se puede ver claramente la palabra “clave” que es la cual se ha establecido como contraseña de ingreso al modo privilegiado de nuestro router.

Para poder establecer una configuración segura con contraseñas encriptados, se puede utilizar el comando “enable secret” de tal manera que se encripta la contraseña ingresada.

Se puede hacer de la siguiente manera:

Jury#conf term

Enter configuration commands, one per line. End with CNTL/Z.

Jury(config)#enable secret clave

Y se podrá ver la encriptación de la contraseña de la siguiente manera

Current configuration: 519 bytes

!

Version 12.4

No service timestamps log datetime msec

No service timestamps debug datetime msec

No service password-encryption

!

Hostname Jury

!

!

!

Enable secret 5 1mERr$OKwHrPttbwvuCNMaqlta9

(Systems, 2012)

Como podemos ver se encripta la contraseña no mostrándola el rato de enseñar el archivo de configuración.

A continuación se aprenderá a proteger las líneas de consola que son las que se muestra el rato del ingreso al router por la interfaz de consola para configuración.

El comando login va a permitir la verificación de la contraseña en la línea de consola, como se muestra a continuación de igual manera se habilitara la contraseña mediante el uso del comando enable password esto se hará de la siguiente manera:

Jury(config)#line console 0

Jury(config-line)#password fiflo

Jury(config-line)#login

(Systems, 2012)

En este momento se va a contar con contraseña antes de ingresar al modo usuario de tal manera que se bloquean las entradas al modo privilegiado y al modo de configuración global. Se ve de la siguiente manera.

Press RETURN to get started.

User Access Verification

Password:

(Systems, 2012)

Como se puede ver se pide una contraseña antes de ingresar al modo usuario, cabe recalcar que de igual manera estas contraseñas no son encriptados todavía.

Se puede hacer lo mismo para el acceso vía telnet, este tipo de conexión establece un tubo no cifrado a través de cualquier medio de transmisión estableciendo conexión con cualquier equipo remoto que lo soporte pero el acceso por este medio como se mencionó anteriormente, se puede proteger con contraseña, bloqueando el acceso en la línea vty con el mismo comando anterior enable password. Se haría de la siguiente manera:

Jury(config)#line vty 0 4

Jury(config-line)#password fiflo

Jury(config-line)#login

(Systems, 2012)

En este momento queda fijada la contraseña para la línea de acceso por telnet.

Pero de igual manera como se mostró anteriormente, estas contraseñas no son encriptados, lo cual deja las conexiones vulnerables a cualquier intromisión por vía WAN como se muestra a continuación.

Current configuration: 542 bytes

!

Version 12.4

No service timestamps log datetime msec

No service timestamps debug datetime msec

No service password-encryption

!

Hostname Jury

!

Enable secret 5 1mERr$OKwHrPttbwvuCNMaqlta9.

Enable password fiflo

Line con 0

Password fiflo

Login

Line vty 0 4

Login

(Systems, 2012)

Como se puede ver en las zonas resaltadas no se encripta las contraseñas anteriormente guardadas. Para hacer esto, se tiene que habilitar el comando “Service password-encryption” de esta manera se logra una encriptación en la asignación de contraseñas guardadas para todas las líneas. Y se verá de la siguiente manera

Jury(config)#service password-encryption

Version 12.4

No service timestamps log datetime msec

No service timestamps debug datetime msec

Service password-encryption

!

Hostname Jury

!

Enable secret 5 1mERr$OKwHrPttbwvuCNMaqlta9.

Enable password 7 082745480516

Line con 0

Password 7 082745480516

Login

Line vty 0 4

Password 7 082745480516

Login

(Systems, 2012)

Como se puede notar, se encuentran encriptados las contraseñas.

Configuración de cada una de las interfaces

Como se explicó anteriormente, existen distintas interfaces dentro del modem, ya sean estas destinadas hacia la WAN o hacia una LAN para lo cual nos guiaremos

con la tabla de direccionamiento de la cual se habló anteriormente. Para esto se seguirán los siguientes pasos.

1.- Ingreso a la línea de la interfaz.

Esto se hace mediante el uso del comando interface como por ejemplo:

```
Jury(config)#interface serial 0/1/0

Jury(config-if)#
```

(Systems, 2012)

2.- Configurar la IP que va en la interfaz tal como está en la tabla de direccionamiento.

Para esto se tiene que haber hecho el subneteo de la red y tener una tabla de direccionamiento lista para ser utilizada. Para motivos de ejemplo se va a usar la IP 192.168.1.1 como IP y una máscara /24 asignada hacia una serial.

Se haría de la siguiente manera:

```
Jury(config-if)#ip address 192.168.1.1 255.255.255.0
```

3.- Darle una descripción al enlace que se hace.

Esto se logra mediante el uso del comando “description” donde en realidad se pone el uso que se le va a dar a la interfaz como por ejemplo esta interfaz es para la conexión a la red 192.168.1.0. Se vería de la siguiente manera:

Jury(config-if)#description conexión a la red 192.168.1.0

4.- Subir la interfaz.

Se puede hacer mediante el uso del comando “no shutdown” lo cual hace que la interfaz suba administrativamente pero no como protocolo, esto solo subirá cuando la interfaz sea conectada. Quedaría así:

Jury(config-if)#no shutdown

5.- Se verifica la configuración

Para esto se hace uso del comando “show ip interface brief”, el cual nos va a indicar el estatus de la interfaz y la IP que tiene asignada al momento.

Jury#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	administratively down	
FastEthernet0/1	unassigned	YES	unset	administratively down	down
Serial0/1/0	192.168.1.1	YES	manual	down	down

Serial0/1/1 unassigned YES unset down down

Vlan1 unassigned YES unset administratively down down

Jury#

(Systems, 2012)

Como se puede ver en el compendio de las interfaces se ve lo que se ha hecho anteriormente.

Algo que no hay que olvidar es que siempre que se utilice una conexión serial, esta tendrá siempre 2 puntas el DCE[19] (equipo de terminación de equipo de datos) y el DTE[20] (equipo terminal de datos) el extremo de DCE va a tener que configurarse el reloj esto solo con las conexiones seriales. Esto se hará mediante el comando "clock rate" de la siguiente manera

Jury(config-if)#clock rate 64000

(Systems, 2012)

Configurar un mensaje de bienvenida

Una forma de darle un toque personal a la configuración del router es el hecho de poder configurar un mensaje de bienvenida o como es conocida en la configuración de MOTD (message of the day) Esto traducido al español es conocido como Mensaje del día el cual puede contener lo se quiera poner como mensaje esto se logra

[19] "Data Communications Equipment", es el proveedor del servicio.
[20] "Data Terminal Equipment", cualquier equipo informático,sea receptor o emisor final de datos.

mediante el comando “banner motd” no olvidar siempre poner al final el caracter con el cual se va a terminar el mensaje de la siguiente manera:

```
Router(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Peligroso no entrar a menos que se tengan los conocimientos debidos#
```

Como se puede observar se termina con el # lo cual indica el final de la configuración del mensaje del día. Aquí se mostrara como se muestra el mensaje del día.

```
%SYS-5-CONFIG_I: Configured from console by console

Peligroso no entrar a menos que se tengan los conocimientos debidos

Router>
```

(Systems, 2012)

Guardar cambios en el router

Como se había mencionado anteriormente hay dos archivos que se manejan dentro de la flash del router, los cuales son el startup config o configuración de inicio que como su nombre lo indica es el archivo de inicio o con el cual inicia el router, y se

tiene el running config que es volátil es decir este se pierde al rato de mandar a reiniciar el router. La forma de guardar los cambios es hacer que el running config se vuelva el startup config mediante el comando "copy running-config startup-config", como se puede ver el comando es "copy inicio destino" sin olvidar el espacio entre los dos de lo contrario se mostraría un error de comandos. Se verá de la siguiente manera:

Router#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Router#

(Systems, 2012)

Verificar la configuración básica

La mejor herramienta que se puede tener para verificar cualquier configuración que se haga dentro de un router es verificar la configuración que se ha hecho, la forma de hacer esto es mediante el comando "show" el cual nos mostrara cualquier archivo de configuración que se desee ver para poder ver la configuración que se ha hecho en el momento solo se tiene que poner "show running-config" y nos saldrá detallado todo lo configurado en el router se vera de la siguiente manera:

```
Jury#show running-config
Building configuration...

Current configuration : 634 bytes
!
Version 12.4
No service timestamps log datetime msec
No service timestamps debug datetime msec
No service password-encryption
!
Hostname Jury
!
!
!
Enable password clave
!
!
!
Interface FastEthernet0/0
 No ip address
 Duplex auto
 Speed auto
 Shutdown
```

!

Interface FastEthernet0/1

No ip address

Duplex auto

Speed auto

Shutdown

!

Interface Serial0/1/0

Description conexión a la red 192.168.1.0

Ip address 192.168.1.1 255.255.255.0

Clock rate 64000

!

Interface Serial0/1/1

No ip address

!

Interface Vlan1

No ip address

Shutdown

!

Ip classless

!

!

Line con 0

Line vty 0 4

Login

!

End

(Systems, 2012)

2.6 Fundamentos de enrutamiento

El enrutamiento o las rutas se establecen para redes no conectadas directamente con el router porque a las redes conectadas directamente se las reconoce automáticamente por lo tanto siempre va a haber ruta hacia ellas. Para redes no conectadas directamente, se tienen dos tipos de enrutamiento los cuales pueden ser:

- Estáticos
- Dinámicos

2.6.1 Enrutamiento estático

Las rutas estáticas se utilizan en las siguientes ocasiones

- Cuando son redes pequeñas compuestas por pocos routers
- Cuando se establece una conexión a internet a través de un único ISP[21]
- Cuando se establece una topología Hub-and-spoke (topología Hub and spoke se denomina cuando se tiene una ubicación central Hub y múltiples

[21] "Internet Service Provider", es una empresa que brinda conexión a Internet a sus clientes.

sucursales también llamadas spokes, donde cada spoke mantiene una conexión con el Hub)

Para establecer un enrutamiento estático se usa el comando “Ip route” el cual usaremos indicando la red de la que sale y el siguiente paso en la ruta hacia el destino de nuestro paquete de datos. Se supondrá para este ejemplo que vamos a partir de la red 192.168.4.0/24 y vamos a hacerlo a través del paso 192.168.2.1 recordando que se quiere alcanzar la red 192.168.1.0 entonces el comando quedará:

```
Jury(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1
```

Una vez que hemos hecho esto comprobaremos la conectividad entre routers haciendo un ping como se verá a continuación

```
Jury#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/31/32 ms
```

(Systems, 2012)

El signo de admiración indica que se tiene éxito en el ping y que se tiene alcance con el siguiente router.

También se puede realizar esto cuando en vez de la IP de destino solo se pone la interfaz por la cual sale la ruta para esto se supondrá para cuestiones de ejemplo que se saldrá a través de la interfaz serial 0/1/0 de este router quedando el comando:

```
Jury(config)#ip route 192.168.1.0 255.255.255.0 serial 0/0/0
```

Se podrá verificar todas las rutas establecidas al momento mediante el uso del comando “show ip route” y se vera de la siguiente manera:

```
Sh 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
```

S 192.168.1.0/24 [1/0] via 192.168.2.1

C 192.168.2.0/24 is directly connected, Serial0/1/0

C 192.168.4.0/24 is directly connected, FastEthernet0/1

(Systems, 2012)

Se podrá observar la letra S en la primera ruta indicando que es una ruta estática mediante la cual la red 192.168.1.0 /24 está conectada mediante el salto 192.168.2.1.

2.6.2 Enrutamiento dinámico

Existen también los protocolos de enrutamiento dinámicos los cuales fabrican la ruta según la métrica y la ocupación de la red a esto se suman los términos que se va a mencionar a continuación:

- Descubrimiento automático de redes
- Actualización y mantenimiento de las tablas de enrutamiento

Descubrimiento automático de redes

El descubrimiento automático de las redes cercanas es la habilidad de un protocolo de enrutamiento para compartir información sobre las redes que posee ya en su tabla de enrutamiento con los otros routers siempre y cuando estos routers utilicen también el mismo protocolo de enrutamiento. De esta forma nos evitamos el estar configurando todas y cada una de las rutas que se van a utilizar.

Actualización y mantenimiento de las tablas de enrutamiento

Una vez que se ha realizado el descubrimiento de una red, se procede a hacer el mantenimiento y actualización de las tablas de enrutamiento, donde en este punto según el protocolo y la red o se envían mensajes en broadcast dentro de la red verificando el estado de los enlaces entre un router y otro. En este proceso se verificaran las redes vecinas y subredes que se mantienen en cada una de las interfaces.

Existen varios protocolos de enrutamiento dinámico los cuales se irá viendo en el desarrollo de esta tesis entre los cuales se tendrá:

- RIP (Routing Information Protocol) en español protocolo de información de ruteo)
- IGRP (Interior Gateway routing protocol)
- OSPF (Open Shortest Path First)
- IS-IS (intermediate System to Intermediate Systems)
- BGP (Border Gateway Protocol)

2.7 Direccionamiento IP

Para recordar, la dirección IP sirve para identificar dispositivos dentro de una red, facilitando así la comunicación en capa 3 del modelo OSI. Está compuesta por 32 bits de manera lógica 1 y 0 (forma binaria), que esta separa por puntos formando 4 octetos y puede ser también representada en forma decimal.

32 BITS

10100111.	**00001111.**	**10001010.**	**10101010**
	OCTETO		

=

DECIMAL

167.	**15.**	**138.**	**170**

Existen rangos para determinar las clases de IP, para facilitar su uso en redes públicas y privadas.

CLASE	PRIMERA IP	ULTIMA IP
A	0.0.0.0	127.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
MULTICAST	224.0.0.0	239.255.255.255
EXPERIMENTAL	240.0.0.0	255.255.255.255

2.7.1 Direcciones de clase A

Usan el primer octeto como dirección de red y dejando así los 3 octetos restantes para uso de host, es decir en clase A se usa para redes extensas ya que se tiene para host una disponibilidad de 16777216 de hosts. Hay que tener en cuenta que la dirección 127.x.x.x se deja reservada para pruebas de loopback.

- Numero de redes: 126
- Numero de host: 16.777.216

2.7.2 Direcciones de clase B

Las direcciones de clases B ocupan los dos primeros octetos para red y dejando así 16 bits para host, se podría decir que esta clase está orientada a redes medianas.

- Numero de redes: 16.384
- Numero de host: 65.534

2.7.3 Direcciones de clase C

Las direcciones de Clases C usan los 3 primeros octetos para dirección de red y el último para host, teniendo de tal manera varias redes de pocos hosts.

- Numero de redes: 2.097.152

- Numero de host: 254

Al momento de usar estas direcciones IP con clase en los protocolos de enrutamiento se estaba desperdiciando espacio IP y por tal motivo se desarrolló VLSM.

2.8 VLSM (Variable Length Subnet Mask)

En la actualidad como se ha estado agotando el direccionamiento IP de manera rápida y se necesitaba un método de asignar el direccionamiento con mayor eficacia, en la que se pueda subdividir una subred, es decir teniendo una dirección 192.168.1.0 se subdivida modificando su prefijo de mascara, como se muestra en la imagen del figura 2. **(Ver Figura 2)**

Ejemplo:

En el caso que se necesite asignar direcciones IP a un enlace Serial se suele solo necesitar dos direcciones IP, pero si se asigna la dirección 192.168.1.0/24 tendremos un total de 254 IPs que no se van a utilizar en su totalidad, aquí viene la función de VLSM, entonces subdividimos la red (**Figura 2**). De tal manera que nos va a quedar la dirección 192.168.1.0 /30, en la cual la primera dirección y la última no son utilizables ya que pertenecen a la dirección de red y broadcast respectivamente.

SUFIJO: 30

RED: 192.169.1.0

HOST: 192.169.1.1

HOST: 192.169.1.2

BROADCAST: 192.169.1.3

2.9 CIDR y rutas resumen.

Se lo suele conocer también como agregación de rutas, es el proceso por el cual las direcciones se unifican y se las representan con una dirección única, teniendo en cuenta que la dirección resumen debe abarcar todas las direcciones que han sido objeto de resumen, optimizando las rutas ya que reduce el tamaño de las tabla de enrutamiento. Ya estos conceptos se han visto en el uso del protocolo RIP estudiado en capítulos anteriores.

Para realizar el resumen de rutas hay que tener presente que deben ser direcciones contiguas para verificar en que bit varían estas direcciones y dependiendo de cuantos bits sean similares, esa cantidad será el prefijo de red. Las superredes no son otra cosa que rutas resumen.

Con estos procesos varía el conocimiento que se tenía con respecto a la dirección de red y el direccionamiento con clase, con el uso del CIDR ahora la duración del

prefijo determina la dirección de red y así mismo se puede lograr el resumen creando una superred.

Así mismo para lograr difundir estas redes subdividas o superredes hay que utilizar protocolos de enrutamiento con clases, ya que los protocolos sin clases necesitan de la máscara de subred y dirección de red para propagar en las actualizaciones periódicas.

Capítulo 3

3 Introducción a Enrutamiento estático

Como se mencionó en el capítulo anterior los routers son los encargados de las transferencias de paquetes a otras redes, importantes el enrutamiento de paquetes a cualquier red de datos y así tener una comunicación de origen al destino en una internetwork.

Los protocolos de enrutamiento pueden ser dinámicos o manuales (estableciendo rutas estáticas), en algunas ocasiones se suele usar una combinación de ambos protocolos de enrutamiento.

Las ventajas del enrutamiento estático es que no requiere de muchos procesos comparado al enrutamiento dinámico, pero es más difícil configurar cuando se tiene gran cantidad de rutas.

3.1 Router y redes

3.1.1 Conexiones

En este proyecto trabajaremos con el Packet tracer[22] como simulación de cómo se va a comportar la red, en el cual vamos a emplear tres routers modelo 1841 equipados con interfaces seriales y se conectara mediante enlaces WAN el de router a router, también cada equipo tendrá una red LAN conectada a un equipo terminal (PC).

Recordando que las conexiones entre routers se harán de por interfaces seriales, cabe indicar que hay diferentes conectores seriales y los routers CISCO pueden trabajar con diferentes estándares como se va a detallar y verificar brevemente:

EIA232

"Es la norma más popular y desarrollada por la EIA (Electronics Industry Association), se da para la conexión de un equipo terminal datos (DTE) y uno de terminación de un circuito de datos (DCE)". (Vargas, 2010)

"Al principio llamada RS-232, pero también suele reconocerse bajo los nombres de RS232, EIA232 y EIA / TIA. **(Ver Figura 1)**" (Gómez, pág. 5)

[22] Herramienta de simulación de redes interactiva para los instructores y alumnos; de propiedad de Cisco Systems.

- Utiliza cable de 25 conductores, pero solo 4 son utilizados para datos y los restantes quedan para temporizar y control. **(Ver Figura 2)**
- Los conectores son DB-25 macho para el DCE (en el caso del router es para el equipo en el cual va configurado el clock rate) y DB-25 hembra que corresponde al DTE

EIA 449

"Así mismo orientada a la conexión entre DCE Y DTE, teniendo como velocidad de transmisión 2Mbps en cables de hasta 60 metros, esta norma utiliza conectores D-sub con 37 y 9 pines. **(Ver Figura 3)**" (Teleproceso, 2010, pág. 3).

V.35

Desarrollada por la ahora llamada ITU[23] es un estándar de transmisión de datos a alta, recordando que usa transmisión síncrona y de velocidades de transmisión de hasta 2 Mbps dependiendo de la distancia. **(Ver Figura 4)**. Los conectores comunes son el DB-35 o el MRAC-34. **(Ver Figura 5)**

[23] "International Telecommunication Union", Organismo internacional de estandarización y normalización de las telecomunicaciones.

Esta norma puede usarse de dos formas: Se usa señales desbalanceadas para control y señalización, al contrario de usar señales balanceadas (baja impedancia[24]) que nos dará para datos y reloj.

X.21

Estándar muy poco usado ya que no permite una gran tasa de transmisión (20 Kbps) a una distancia máxima de 15 metros, generalmente usado para enlaces punto a punto y utiliza conectores DB-25 para interconexión de DTE-DCE

Para los que son conexiones LAN se usara cables UTP[25] categoría 5E, ponchados a conectores RJ45, tendiendo en cuenta que las configuraciones que existen son 2: conexión directa y cruzada.

Para la conexión directa es básicamente cuando se conectan equipos diferentes y como por ejemplo: Swicth-PC, Router Switch. Se usa el estándar T568A. "**(Ver Figura 6)"** (rodri.wordpress.com, 2007)

Para la conexión Cruzada es cuando se conectan equipos de las mismas características como: PC-PC, Router-Router y se usa el estándar T568A en un extremo y el T568B. **(Ver Figura 7)**

[24] Obstrucción u oposición al paso o al flujo.
[25] "Unshielded Twister Pair", Par trenzado no apantallado, uno o más pares de cable rodeados por un aislamiento.

3.2. Configuración de interfaces

3.2.1 Configuración y verificación de una interfaz Ethernet

Para introducirnos a lo que respecta sobre el enrutamiento estático, veremos brevemente las configuraciones básicas del router necesarias para que las interfaces que van a enviar datos, primero debemos siempre tener en cuenta que las interfaces FastEthernet que vayamos a usar deben estar activas ya que por defectos las interfaces , para esto se usa el comando “NO SHUTDOWN”, para la configuración de una interfaz, primero debemos ingresar al modo de configuración en el router en donde se va a poder asignar la dirección IP de dicha interfaz, como explicaremos a continuación:

```
Router# configure terminal
Router# interface FastEthernet 0/1
Router# ip address 192.168.0.1 255.255.255.0
Router# no shutdown
```

(Systems, 2012)

Al ejecutar dicho comando ya la interfaz FastEthernet[26] se encontrara activa y con una dirección IP y se presentara una notificación de estado de la interfaz, para poder verificar la tabla de enrutamiento, ingresamos el comando “show ip route” en el cual podremos notar que se encuentra conectado de manera directa y muestra la IP que ha sido configurada.

[26] Ethernet de alta velocidad, siendo ésta 10 veces mayor que la del ethernet normal.

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 not set

C 192.168.0.0/24 is directly connected, FastEthernet0/1

(Systems, 2012)

Para verificar el estado de la interfaz se lo puede realizar con los comandos ya mencionados en el capítulo anterior, entro los cuales tenemos: show interfaces FastEthernet, show ip interface brief, show running config

Se debe tener en cuenta que las interfaces debes estar configuradas en distintas direcciones de red, esto quiere decir que si ya tenemos la FastEthernet 0/1 con la red 192.168.0.1/24, la interfaz FastEthernet 0/0 deberá pertenecer a otro rango de Ip, caso contrario mostrara una error al momento de tratar configurar.

3.2.2 Configuración de una interfaz serial

Para configurar una interfaz serial es el mismo procedimiento que la de una Ethernet, lo que debemos tener en cuenta que para que la línea de protocolo se active (up), se debe tener configurado ambos extremos, ya que si alguna de la interfaz se encuentra Down, la línea del protocolo no cambiara su estado, adicionalmente se debe tener en cuenta que se conectara dos equipos CISCO[27] (equipos DTE), el cual uno hará como DCE y solo en ese equipo deberá configurarse el temporizador con el comando clock rate para el funcionamiento correcto del enlace. A continuación se dará un ejemplo de la configuración de la interfaz serial:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#description red 192.168.1.0
Router(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Router(config-if)#clock rate 56000
```

(Systems, 2012)

[27] Cisco Systems es una empresa principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones

Como se puede verificar el estado sigue Down a pesar de que se ingresó el comando no shutdown, esto pasa porque el otro equipo (DTE) Router2 aún no ha sido configurado. Tener en cuenta que las dos interfaces (DCE-DTE) deben pertenecer a la misma red.

```
Router2#enable
Router2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#interface serial 0/0/0
Router2(config-if)#ip address 192.168.1.2 255.255.255.0
Router2(config-if)#description red 192.168.1.0
Router2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
```

(Systems, 2012)

Como se puede observar en las notificaciones, una vez que los dos routers se encuentren configurados de manera correcta, la línea de protocolo ya estará UP, para verificar la conectividad se puede realizar un ping

Ping desde “Router” a “Router2”

Router#ping 192.168.1.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 2/4/12 ms

(Systems, 2012)

Para ver cuál es el Router que está haciendo como DCE se puede ejecutar el command **show controllers**.

Router# show controllers serial 0/0/0

Interface Serial0/0/0

Hardware is PowerQUICC MPC860

DCE V.35, clock rate 56000

Idb at 0x81081AC4, driver data structure at 0x81084AC0

SCC Registers:

General [GSMR]=0x2:0x00000000, Protocol-specific [PSMR]=0x8

Events [SCCE]=0x0000, Mask [SCCM]=0x0000, Status [SCCS]=0x00

Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E

(Systems, 2012)

Así mismo, al correr el comando **show ip route**, en el listado ya aparecerá en la tabla de enrutamiento la red 192.168.1.0/24 conectada directamente en la serial 0/0/0.

Router#show ip route

C 192.168.0.0/24 is directly connected, FastEthernet0/1

C 192.168.1.0/24 is directly connected, Serial0/0/0

(Systems, 2012)

3.3 Exploración de redes conectadas directamente

Tabla de enrutamiento

Como es de nuestro conocimiento el router envía paquetes de datos a red de destino, el router examina en la tabla de enrutamiento por cual interfaz o siguiente salto seria optimo enviar el paquete, entonces la tabla de enrutamiento no es más que una base de datos que almacena información acerca de las rutas conectadas directamente o ya pueden ser también remotas (Ver **Figura 8**). El principal inconveniente que hay que evitar son los bucles de enrutamiento ya que podría crear un loop infinito y afectaría la convergencia de la red.

Para las redes remotas se pueden añadir rutas de manera manual, pero en redes muy extensas esto resultaría muy molestoso y dependería solo del administrador de la red, para solucionar esto se puede usar enrutamiento dinámico que se actualizaría con cualquier fallo o modificación que sufra la red, esto lo veremos en otro capítulo.

Para la estructura de la tabla de enrutamiento hay que tener en cuenta los siguientes 3 principios (tomados de la currícula de Cisco):

1. "Cada router toma su decisión por sí solo según la información que tenga en su propia tabla de enrutamiento". Cada router se basara en la información que contenga en su propia tabla de enrutamiento, esto quiere decir que no intercambiara información con la tabla de rutas de otro router.

2. "El hecho de que un router tenga cierta información en su tabla de enrutamiento no significa que los demás routers tengan la misma información".

3. Principio 3: "La información de enrutamiento sobre una ruta desde una red hacia otra no brinda información de enrutamiento sobre la ruta inversa o de regreso".

Protocolo de descubrimiento de Cisco. (CDP).

Este es un protocolo propio de Cisco que actúa en la capa 2 (enlace de Datos) del modelo OSI, intercambia información de con equipos que se encuentren conectados de manera directa, envía cabeceras CDP cada 60 segundos, eficaz para enrutamiento de baja de demanda. Cabe recalcar que solo es para equipos Cisco y admite varios protocolos de la capa de red

3.4 Rutas estáticas

Este es un método muy fácil de configurar tal como se lo señalado anteriormente para redes simples y sobretodo en redes que tiene una entrada y salida (red única), esta configuración se irá configurado la ruta manualmente al destino por el administrador, esto es lo que dificultaría en redes de mayor escala ya que sería más propenso a omitir alguna ruta, algún fallo o cambios en la topología.

En la topología de ejemplo podemos ver que Router no llegaría hasta la red LAN de router2, ni a la red LAN de Router3, para esto usaremos el enrutamiento estático con el comando ip route y su sintaxis será la siguiente:

Ip route *"dirección IP" "Mascara de subred" [interfaz de salida o Dirección Ip de siguiente salto]*

En donde la dirección IP es la dirección de red de destino y su respectiva mascara, en él lo que respecta a la interfaz de salida se detallara por cual interfaz saldría los paquetes hacia la red de destino o también se puede usar la dirección IP del siguiente salto, por recomendación es preferible detallar la interfaz de salida ya que por la dirección IP se usaría más recursos del router en encontrar por cual interfaz estaría dicha IP.

Ejemplo de configuración:

Procederemos a realizar en enrutamiento estático del equipo **Router:**

- Ruta estática para LAN de Router2:

  Router#config term
  Enter configuration commands, one per line. End with CNTL/Z.
  Router(config)#ip route 192.168.2.0 255.255.255.0 serial 0/0/0

- Ruta estática para serial Router2-Router3:

  Router(config)#ip route 192.168.3.0 255.255.255.0 serial 0/0/0

- Ruta estática para LAN Router3:

  Router(config)#ip route 192.168.4.0 255.255.255.0 serial 0/0/0

Si nuevamente revisamos la tabla de enrutamiento, veremos que aparecerán las rutas previamente configuradas con la letra S (static) que quiere decir que es una ruta estítica añadida y también detalla cual es la interfaz de salida que para este caso es la serial 0/0/0.

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 not set

C 192.168.0.0/24 is directly connected, FastEthernet0/1

C 192.168.1.0/24 is directly connected, Serial0/0/0

S 192.168.2.0/24 is directly connected, Serial0/0/0

S 192.168.3.0/24 is directly connected, Serial0/0/0

S 192.168.4.0/24 is directly connected, Serial0/0/0

(Systems, 2012)

Así mismo se realizaría el mismo procedimiento en Router2 y Router3, teniendo en cuenta que las rutas que no conocen son las siguientes:

Router2: Red LAN de Router, Ni red LAN Router3.

Router3: Red LAN Router2, red serial Router2-Router, Ni red LAN Router.

Como observación, es preferible configurar las rutas estáticas con la interfaz de salida para redes punto a punto seriales, ya que solo hará un proceso al buscar la interfaz en la tabla de enrutamiento, pero para redes con Ethernet como interfaz de salida se sugiere especificar en la configuración tanto la interfaz de salida como la IP de siguiente salto para que no haya ningún problema en la red recordando que en la interfaz Ethernet se puede encontrar varios dispositivos diferentes conectados que estén en el mismo sitio de red (routers, hosts).

Eliminar o cambiar una ruta estática.

Por alguna necesidad (ruta eliminada) o cambio de topología se necesite eliminar o cambiar alguna ruta estática, se procedería a usar el comando "**no ip route**".
Para ejemplo vamos a eliminar la ruta estática 192.168.4.0/24 en Router que está configurada en la interfaz de salida serial 0/0/0:

Router(config)#**no ip route** 192.168.4.0 255.255.255.0 serial 0/0/0

Y la modificaremos por la IP del siguiente salto que para ejemplo seria la 192.168.2.2 (interfaz serial 0/0/0 de Router2):

Router(config)#ip route 192.168.4.0 255.255.255.0 192.168.2.2

Si verificamos en la tabla de enrutamiento de Router, veremos que ahora aparecerá la nueva ruta estática con la IP de siguiente salto.

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 not set

C 192.168.0.0/24 is directly connected, FastEthernet0/1
C 192.168.1.0/24 is directly connected, Serial0/0/0
S 192.168.2.0/24 is directly connected, Serial0/0/0
S 192.168.3.0/24 is directly connected, Serial0/0/0
S 192.168.4.0/24 [1/0] via 192.168.2.2

(Systems, 2012)

Recordemos como para poder verificar las rutas estáticas configuradas se puede contar con los comandos:

- Show running config
- Show ip route
- Ping, sobre todo este comando nos permite comprobar si los paquetes se están enviando al destino.

Rutas de resumen

La ruta de resumen nos permite reducir la tabla de enrutamiento lo cual nos dará un funcionamiento eficiente a la hora de determinar la interfaz por la cual se enviara el paquete ya que habrá menos información (rutas) por buscar en la tabla.

Por ejemplo si tenemos varias direcciones como: 172.16.1.0/16, 172.16.2.0/16, 172.16.3.0/16, 172.16.4.0/16, 172.16.5.0 y todas usando la interfaz serial 0/0/0, se puede decir que la ruta resumen para este grupo de direcciones, seria: 172.16.0.0/21

Para calcular la ruta se lo hace de la siguiente manera:

- Se escriben las rutas en binario

172.16.1.0 → 10101100.00010000.00000001.00000000

172.16.2.0 → 10101100.00010000.00000010.00000000

172.16.3.0 → 10101100.00010000.00000011.00000000

172.16.4.0 → 10101100.00010000.00000100.00000000

172.16.5.0 → 10101100.00010000.00000101.00000000

- Se empieza desde el bit[28] de la izquierda y se va moviendo hacia la derecha hasta poder notar que los bits ya no coinciden, justo ahí nos detenemos ya que estaríamos en el límite del resumen.

10101100.00010000.00000**001.00000000**

10101100.00010000.00000**010.00000000**

10101100.00010000.00000**011.00000000**

10101100.00010000.00000**100.00000000**

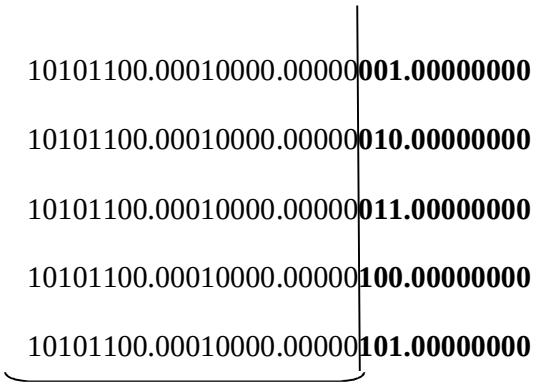
10101100.00010000.00000**101.00000000**

Bits de coincidencia

- Se cuenta los bits del lado que coinciden y eso nos dará la máscara de subred para la ruta de resumen.

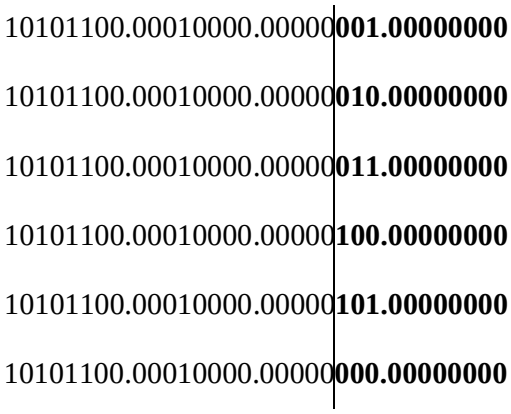
[28] "Binary digit", Un número binario codificado como dato. Un bit puede ser un “uno” o un “cero”.

22 bits de coincidencia



Mascara de subred: 255.255.255.248

- Para identificar la dirección de red simplemente se copian todos los bits que coinciden y en los demás se pone 0 hasta completar los 4 octetos de bits.



Dirección de red: 172.16.0.0

Para configurar una ruta estática de resumen se realiza el mismo proceso como se ha indicado anteriormente, recordando que la ruta resumen abarca lar direcciones antes mencionadas, ejemplo:

Ip route 172.16.0.0 255.255.255.248 [interfaz de salida o IP de siguiente salto]

Ruta por defecto.

La ruta por defecto es usada para toda ruta que no coincida con una ruta estática, los paquetes se envíen al siguiente salto, esto es comúnmente usado para cuando se tiene un ISP para enviar todo el tráfico hacia el ISP (parecido a un Gateway) o cuando hay una conexión única hacia otro router. "**(Ver Figura 9)"** (Cisco Systems, 2009)

El comando será el mismo ip route, pero la dirección de red y mascara será la quad zero (0.0.0.0) ejemplo:

Ip route 0.0.0.0 0.0.0.0 [Ip siguiente salto – Interfaz de salida]

Esto nos permite que en vez de tener guardadas rutas de todas las redes, se tenga una por defecto para las rutas que no aparezcan en la tabla de enrutamiento.

Capítulo 4

4 Introducción enrutamiento dinámico

En capítulos anteriores vimos la base del ruteo donde se ha aprendido ruta estática como establecer las cosas se prendió lo que es enrutamiento estático en el router y las bases de una ruta estática por las rutas por defecto los capítulos anteriores o institución protocolos de enrutamiento dinámico incluso como se clasifican diferentes protocolos de enrutamiento.

Los protocolos para enrutamiento dinámico son utilizados en redes de tamaños grandes tamaños mayores para facilitar la saturación del administrador de red y la operatividad del mismo. El uso de solo rutas estáticas implica mucho esfuerzo para el administrador de red, sobre todo con el crecimiento de la misma, se crean los protocolos dinámicos tocó los de enrutamiento dinámico para poder lograr una mejor utilización de la red.

Hace muchos años a principios de la década del 80 aproximadamente han surgido varios protocolos de enrutamiento dinámico. Este capítulo se analizará características y diferencias entre estos protocolos de enrutamiento.

4.1 Perspectiva e información básica

Los protocolos de enrutamiento dinámico ácidos dejados en redes desde los comienzos de la década de los 80. La primera presión de RIP se lanzó en 1982, ver algunos de los algoritmos básicos dentro del protocolo que se usaban en ARPANET[29] en 1969.

Debido a la evolución de las redes ya su complejidad cada vez mayor han surgido nuevos protocolos de enrutamiento.

Una de las primeras protocolo enrutamiento fue Routing Information Protocol (RIP). Routing Information Protocol ha evolucionado a una nueva versión tenemos el RIP v2 sin embargo la versión más nueva de RIP l aún no llega a escala de redes más extensas. Para lograr llegar a redes más extensas se desarrollaron dos protocolos de enrutamiento avanzados uno de ellos eran Open Shortest Path First o también llamado OSPF y el Intermediate System to Intermediate System (IS-IS). Después de un tiempo se creó el Interior Gateway Routing Protocol (IGRP) y su evolución el Enhaced IGRP (EIGRP), ambos protocolos desarrollados por Cisco Systems y

[29] "Advanced Research Projects Agency Network", Red americana de los años sesenta. Se considera el origen de Internet.

propiedad intelectual de cisco, protocolos que fueron diseñados para trabajar en redes amplias.

Publicó anteriormente en este capítulo se estudiará el funcionamiento de los protocolos de enrutamiento dinámico ahora viene la interrogante ¿qué son exactamente los protocolos de enrutamiento dinámico? Los protocolos de tratamiento dinámico se utilizan mayormente para compartir información en forma dinámica sobre redes remotas aire formando automáticamente información acerca de cada uno de los equipos de la red dentro de sus tablas enrutamiento.

Los protocolos enrutamiento siempre van a terminar la mejor ruta a cada red que luego se va agregando una hacia la tabla de enrutamiento. Una de las principales ventajas de usar enrutamiento dinámico es que si la topología de la red cambia sea cual sea el motivo este se registra automáticamente dentro de la tabla de enrutamiento que tal manera que se algún enlace que es el bar dentro de la red siempre se buscará una ruta alterna buscando siempre la mejor métrica para lograr llegar hacia el usuario final logrando así una comunicación estable sin pérdida de paquetes.

A diferencia del protocolo enrutamiento estático los protocolos de enrutamiento dinámico requieren de menos sobrecarga administrativa. Un factor bastante importante dentro del uso de enrutamiento dinámico es que hay que dedicar cierta parte los recursos de un router para la operación de un protocolo. Incluso el tiempo

del procesador al procesar un paquete y el ancho de banda que se requiere para el enlace de la red es mucho más grande. Esto hace que utilizar un protocolo enrutamiento dinámico sea siempre un poco más complicado de elegir pues se tiene que decidir entre rapidez al procesar un paquete y la carga administrativa es decir, la carga que se le da a un administrador de red al rato de realizar una ruta estática, sin embargo la ruta estática en cambio no se puede tomar en cuenta los cambios que se dan dentro de la red lo cual hace que si un enlace se cae automáticamente este paquete se pierda , no se mantiene una ruta nueva como se lo hace con los protocolos de enrutamiento dinámico dentro de las cuales las rutas van cambiando según el uso de la red y la evolución de la misma.

4.1.1 Descubrimiento de redes y mantenimiento de la tabla de enrutamiento

Propósito de los protocolos de enrutamiento

Un protocolo es una serie de reglas que se le da un paquete para poder llegar a un usuario final un protocolo de enrutamiento es un conjunto de procesos algoritmos y mensajes que se usa para poder escoger la por rutas de protocolo de enrutamiento dependiendo el emulsión de la red y la métrica que existe la misma. Los propósitos de un protocolo de enrutamiento son:

- Descubrir redes remotas
- Mantener la información de rutas actualizado

- Seleccionar la mejor ruta hacia redes de destino verificando siempre la métrica
- Capacidad de buscar una mejor ruta en caso de falla de algún enlace.

Componentes de un protocolo de enrutamiento

1.- Estructura de datos: Los protocolos de enrutamiento utilizan tablas o base de datos para sus operaciones dentro de la red. Cierta parte de información se guarda dentro de la RAM del ruteador.

2.- Algoritmo: como se pudo haber definido anteriormente algoritmo una lista limitada de pasos que se utilizan para poder llevar a cabo la tarea. protocolo enrutamiento utilizan efectivamente los pasos de cuales encuentran dentro de su programación para poder desarrollar lo que es la inteligencia de protocolo, de esta manera siempre se valora poder establecer la mejor ruta para un paquete.

3.- Mensajes del protocolo de enrutamiento: Los protocolos de enrutamiento utilizan múltiples tipos de anuncios o mensajes para poder encontrar routers externos de esta manera intercambia información de enrutamiento y otras tareas para aprender conservas y poder implementar nueva información de la red.

Operación de un protocolo de enrutamiento dinámico

La gran mayoría de protocolo enrutamiento tienen un mismo propósito el cual es conocer acerca de redes remotas y adaptarse rápidamente a cambios en la topología de la red. El método que utiliza un protocolo para lograr su propósito depende del algoritmo con el cual fue programado y las características operativas de este protocolo. La operación protocolo enrutamiento dinámico varía según el tipo de protocolo el protocolo de enrutamiento en sí. Generalmente la operación un protocolo dinámico puede describirse como se muestra a continuación:

El router envía y recibe mensaje de enrutamiento en sus interfaces

Un router comparte mensajes de información de enrutamiento con otro router o redes externas que están operando dentro del mismo protocolo enrutamiento es muy importante siempre recordar que ambos tienen que sincronizarse con el mismo protocolo

Los routers intercambian información de enrutamiento para poder aprender acerca de redes aledañas.

Cuando se detecta un cambio en la topología de la red el router tiene que adaptarse a los cambios de la red utilizando una ruta externa una ruta alterna para poder enviar un paquete.

4.1.2 Ventajas y desventajas Enrutamiento estático.

Si algo se puede dejar claro en este capítulo es que el enrutamiento estático se utiliza para redes pequeñas, las cuales no se han previsto para PC significativamente debido a esto tendrá en cuenta las siguientes ventajas:

Facilitar el mantenimiento de la tabla de enrutamiento en redes pequeñas las cuales no se ha previsto que crezcan en manera significativa

Debido a ser redes pequeñas el tratamiento desde y hacia las redes de conexión es único.

El uso de una sola ruta estática por defecto puede representar la ruta hacia cualquier red q no tiene la coincidencia más específicas con otra ruta en la tabla de enrutamiento.

Como se había indicado anteriormente el uso de la CPU del router es mucho menor

Es mucho más sencillo para que un administrador de red comprenda la tabla de enrutamiento

Dependiendo del punto de vista y el tamaño de la red una ruta estática siempre es mucho más sencilla de configurar.

Desventajas

Configuración de rutas estáticas en un poco complicada siempre cuando pues estamos hablando de redes grandes recordando que cada subred dentro de la LAN va a necesitar una ruta estática hacia la WAN.

Debido a que es enrutamiento no es orientado hacia redes grandes redes que proyectan crecer la configuración propensa a errores.

Se requiere la intervención del administrador de red para poder cambiar la ruta en caso de algún cambio la topología lo cual implica y si existe algún daño un enlace en

algún momento dentro de la red el administrador de red tendrá que intervenir para hacer cambios en la ruta.

Requiere de toda la eficacia y la pericia del administrador de red para que esta configuración estática se pueda implementar de manera correcta ya que el administrador de red deberá de saber toda la topología de la red.

4.1.3 Ventajas y desventajas del enrutamiento dinámico

4.1.3.1 Ventajas

Se facilita el trabajo realizado de red pues ya no se tiene que está programando ruta estática para cada una de las redes dentro de la LAN.

Los protocolos están constantemente monitoreando la red y verificando a un cambio que ayer su topología de esta manera siempre ratones comunicación entre un punto y otro.

Este tipo de configuración por su naturaleza es mucho menos propensa a errores, debido a que un protocolo evoluciona según la red esto indica que efectivamente no importará si la red crece o no porque esté siempre verificará y monitorear a la red para poder terminar la mejor ruta.

4.1.3.2 Desventajas

Debido a la inteligencia de los protocolos protocolo suele empezar por sus algoritmos bastante lo cual implica que se utilizan recursos del router tales como la CPU, procesamiento y ancho de banda.

El administrador requiere por naturaleza del protocolo de tener más conocimiento de cada uno de ellos, como trabajan, su configuración para poder hacer verificaciones y poder dar solución a los problemas que se den dentro de la red.

Los protocolos de enrutamiento se pueden clasificar en distintas agrupaciones según sus características y su inteligencia, los protocolos de enrutamiento dinámico que más se utilizan son los siguientes:

- RIP: (Routing Interior Protocol).
- IGRP: (Interior Gateway Routing Protocol).
- OSPF: (Open Shortest Path First).
- ISIS: (Intermidiate System to Intermidiate System).
- EIGRP: (Enhaced IGRP).
- BGP: (Border Gateway Protocol).

4.2 IGP y EGP

Un sistema autónomo es un sistema de routers que se encuentran regidos por una administración común. Un ejemplo de una red autónoma es el sistema de red de una empresa que maneja enlaces intersucursales, estas empresas manejan routers para poder determinar la mejor ruta dentro de esta topología, debido a que internet se basa en sistemas autónomos se requieren protocolos de enrutamiento para poder manejarse tanto a la LAN como hacia la LAN es decir protocolos de enrutamiento interior y exterior.

Para estos casos se utiliza

IGP (interior Gateway Protocol) se utilizan para sistemas intrautónomos es decir enrutamiento dentro de sistemas autónomos.

EGP (Exterior Gateway Protocol) se utiliza para enrutamiento de sistemas interautonomos, es decir, enrutamiento entre sistemas autónomos.

4.3 Vector distancia y estado del enlace

Los protocolos de enrutamiento de sistemas intrautónomos de Gateway interior también llamados IGP se clasifican de la siguiente manera

- Protocolos por vector distancia
- Protocolos por estado de enlace

Protocolos de enrutamiento por vector distancia

Al referirnos a vector distancia se está hablando de lo que se llamara de ahora en adelante **métrica**, la métrica es la distancia expresada en saltos y dirección que se tiene de un punto a otro siempre se va a escoger la ruta que tiene el menor número de saltos. Los protocolos de enrutamiento que toman en cuenta el vector distancia se basan en el algoritmo de Bellman-Ford para calcular la métrica y la determinación de la mejor ruta.

Ciertos protocolos por vector distancia hacen un refresh de sus tablas de enrutamiento es decir se envían de forma periódica de un punto a otro de la red, de esta forma se da a conocer los vecinos conectados a un router, en redes bastante grandes esto puede transformarse en una desventaja pues por lo extenso de las redes la tabla de enrutamiento tiende también a serlo lo cual puede llegar a causar trafico excesivo dentro de la red y hasta saturación de enlaces.

Profundizando un poco acerca del algoritmo de Bellman- Ford

El algoritmo de Bellman-Ford (algoritmo de Bell-End-Ford), genera el camino más corto en un Grafo dirigido ponderado (en el que el peso de alguna de las aristas puede ser negativo). El algoritmo de Dijkstra resuelve este mismo problema en un tiempo menor, pero requiere que los pesos de las aristas no sean

negativos. Por lo que el Algoritmo Bellman-Ford normalmente se utiliza cuando hay aristas con peso negativo. Este algoritmo fue desarrollado por Richard Bellman, Samuel End y Lester Ford.

Según Robert Sedgewick, “Los pesos negativos no son simplemente una curiosidad matemática; surgen de una forma natural en la reducción a problemas de caminos más cortos” (YAMID, 2010), y son un ejemplo de una reducción del problema del camino hamiltoniano que es NP-completo hasta el problema de caminos más cortos con pesos generales. Si un grafo contiene un ciclo de coste total negativo entonces este grafo no tiene solución. El algoritmo es capaz de detectar este caso.

Si el grafo contiene un ciclo de coste negativo, el algoritmo lo detectará, pero no encontrará el camino más corto que no repite ningún vértice. La complejidad de este problema es al menos la del problema del camino más largo de complejidad NP-Completo.

De lo que podemos recopilar que este algoritmo siempre tomara en cuenta para calcular la mejor ruta mediante un costo en saltos para llegar de un lado al otro. De esta manera se verifica y se calcula la métrica.

Los protocolos por vector distancia utilizan a los routers como letreros para poder llegar de un punto a otro de esta forma se determina el alcance de un punto a otro

de la red, cabe recalcar que los routers no tienen un mapa de la red se determina armando las rutas verificando la información de los routers vecinos.

Los protocolos por vector distancia funcionan de mejor manera cuando

El diseño de la red es jerárquico, esto por lo general ocurre en redes extensas.

El administrador tiene pleno conocimiento del funcionamiento del protocolo.

4.4 Protocolos con clase y sin clase

4.4.1 Protocolos con clase

Los protocolos con clase no envían información de la máscara de subred en cada una de las actualizaciones enviadas en el enrutamiento, los primeros protocolos de enrutamiento dinámico como RIP, fueron protocolos con clase, en esos tiempos las direcciones de red ip se asignaban con diferentes clases; clase A, B o C. No era necesario el envío de la máscara ya que la máscara podía determinarse por el primer octeto de la dirección de red.

Estos protocolos aún pueden utilizarse en redes actuales pero dado a que no se utiliza la máscara de subred no se puede utilizar en redes que mantienen redes

subneteadas pues no se actualiza a que subred iría pues se juega en el subneteo con los octetos sin importar la clase.

Los protocolos de enrutamiento con clase incluyen a RIP v1 y a IGRP

4.4.2 Protocolos de enrutamiento sin clase

Son el inverso de los protocolos con clase, es decir, se envía información de la máscara de subred en las actualizaciones enviadas para el enrutamiento sin importar la clase de la dirección de red, lo cual indica que las redes en la actualidad ya no se asignan en función de clases por el subneteo y la máscara de subred no puede determinarse por el primer octeto de la dirección de red, la gran mayoría de redes requieren del método VLSM [30] para poder determinar la expansión de la red.

Los protocolos de enrutamiento sin clase son RIP v2, EIGRP, OSPF y BGP

[30] "Variable Length Subnet Mask", Las máscaras de subred de tamaño variable representan otra de las tantas soluciones que se implementaron para el agotamiento de direcciones ip.

4.5 Convergencia

En capítulos anteriores se ha hablado de la convergencia se estableció que la convergencia es la comunicación entre una red y otra, es decir cuando una red se puede ver con otra técnicamente se tiene que convergencia en enrutamiento dinámico ocurre cuando las tablas de enrutamiento dinámico se encuentran en estado de uniformidad es decir coincide y se tiene toda la información de la red, lo cual indica que se tiene alcance con todas las redes y subredes dentro del enrutamiento.

Las propiedades de la convergencia incluyen también la velocidad de propagación del paquete y el cálculo de rutas óptimas.

4.6 Métricas

4.6.1 Propósito de la Métrica

Como se mencionó anteriormente la métrica es la medida que utiliza el router para la toma de decisiones al rato de escoger una ruta, por lo cual el cálculo de la métrica de la red es muy importante. Generalmente el router aprende más de una ruta hacia el mismo destino pero al rato de elegir la ruta siempre se va a tomar en cuenta la cantidad de saltos que se tienen de un punto a otro o el costo de envío en cada

enlace todo esto se configura y se toma en cuenta para que el router tome la decisión al momento de enviar un paquete hacia la red.

Más adelante se profundizara acerca del cálculo de la métrica y la forma de establecer las reglas para el cálculo de la misma.

4.6.2 Métricas aplicadas a protocolos de enrutamiento dinámico

4.6.2.1 Parametrización de métrica

Como se explicó anteriormente los protocolos de enrutamiento dinámico toman en cuenta la métrica para enrutar un paquete pues siempre se va a buscar el camino que represente menor cantidad de saltos y/o costo dentro de una red, este parámetro también llamado métrica es tomado en referencia de distinta manera según el protocolo de enrutamiento lo cual indica que dos protocolos de enrutamiento dinámico distintos no siempre van a tener la misma ruta entre un punto y otro , se pone en claro que esto depende y dependerá de cómo el protocolo de enrutamiento dinámico tome la métrica en una red.

En RIP siempre se escogerá como métrica prioritaria a la menor cantidad de saltos mientras por ejemplo en OSPF se tomará en cuenta el enlace con el ancho de banda más alto.

Anteriormente se indicó que existían varios criterios a tomar en cuenta en el cálculo de la famosa métrica los cuales son:

1. Conteo de saltos:

   Este tipo de métrica es una métrica simple y sencilla solo se toma en cuenta el número de routers, o también llamados saltos que se tienen entre dos puntos convergentes de la red, es decir; se verificara en la tabla de enrutamiento del router siguiente hasta armar la ruta hacia el destino del paquete y la ruta que tenga la menor cantidad de saltos es la escogida.

2. Ancho de Banda:

   Para poder describir este tipo de métrica es necesario primero preguntarnos ¿Qué es el ancho de banda? Respondiendo a esta pregunta el ancho de banda es la cantidad de información y datos que se puede enviar a través de un enlace en una determinada cantidad de tiempo, entonces se puede concluir que la métrica por cálculo de ancho de banda siempre se va a escoger la ruta que nos del mayor ancho de banda en los enlaces para poder enviar la mayor cantidad de datos posibles en un enlace. A esto se le puede agregar la medida del paquete para poder optimizar el uso de la red de tal manera de que paquetes que tengan o requieran de un ancho de banda menor utilizaran la ruta que ajuste a su ancho de

banda pero esto se puede configurar según el protocolo de enrutamiento dinámico establecido

3. Carga:

Para motivos de explicación de este parámetro de métrica es necesario describir lo que significa el término tráfico, se conoce como tráfico de la red a la ocupación que se tiene en un enlace esto se verifica mediante el paso de datos , carga o tráfico son parámetros parecidos pero no iguales carga es el trabajo y la cantidad de paquetes que cruzan por este enlace pero se determina mediante un estudio de tráfico constante para determinar este parámetro por lo tanto siempre se va a escoger la ruta con menor carga o tráfico para él envió de un paquete de datos.

4. Retardo

El retardo o latencia es como su nombre lo dice el retraso o cuando un paquete llega tarde de adentro de la red a su destino por cualquiera que sea el motivo este es un factor que se mide en tiempo al tener en cuenta este parámetro siempre se escogerá el enlace que me presente la menor cantidad de latencia[31] o retardo.

[31] Se denomina latencia a la suma de retardos temporales dentro de una red.

5. Costo

Anteriormente se mencionó que también se puede establecerla métrica con prioridad de costo del enlace y al hacer esto, seguramente se debe de haber planteado la pregunta ¿A qué se refiere con costo? Pues respondiendo a esta pregunta no siempre los enlaces de los routers se encuentran dentro de una red que nos pertenece esto no solo se da en las redes de datos sino también en las redes móviles como en las redes de telefonía celular de distintas operadoras donde se paga una taza por utilización de ancho de banda de redes aledañas no propias y estas solo se utilizan cuando en realidad no hay otra opción para conectarnos con esta red pero cada enlace tiene su ancho de banda asignada y por ancho de banda y por el enlace en si es el costo. Esto se trae a colación en el aprendizaje de los protocolos de enrutamiento ya que el administrador de red puede establecer dentro del IOS del router un costo establecido por enlace de esta manera se suman los costos por saltos y se va a escoger la ruta que tenga el menor costo.

4.6.3 Balanceo de Carga

Se mencionó anteriormente los parámetros para el cálculo de la métrica pero que sucede cuando hay dos rutas con la misma métrica. En este punto el router va a aplicar algo que se llama balanceo de carga mediante la cual se verificara y se

enviaran los paquetes dentro de la red a través de dos rutas distintas con la misma métrica.

Una forma de comprobar esto es simplemente buscando en la tabla de enrutamiento del router y ver si hay dos rutas con la misma métrica el balanceo de cargas se activa automáticamente.

4.7 Distancias administrativas

4.7.1 ¿Por qué la distancia Administrativa?

Se sabe que los routers aprenden acerca de los routers adyacentes o que están conectados de manera cercana.

En muchos casos es posible que sobre una misma red de destino se tenga información de múltiples orígenes. Por ejemplo, que para una red descubierta por RIPv2, simultáneamente haya sido descubierta por OSPF y que además contemos con una ruta estática.

En estos casos ¿Cuál es la información que privilegia el algoritmo de selección de la mejor ruta para definir la ruta que el dispositivo utilizará para encaminar el tráfico hacia ese destino?

Para dar un parámetro de base para esta toma de decisiones, Cisco IOS asocia a cada ruta un parámetro denominado Distancia Administrativa que le permite identificar el origen de esa información de enrutamiento.

"La distancia administrativa es un número que está en el intervalo de 0-255 el cual se le asigna para dar la confiabilidad del enlace dentro de la red, cuanto menor es el valor, mayor se da la preferencia para elegibilidad de la ruta." (Gerometta, 2010)

Una distancia administrativa de 255 indica que el enlace no es confiable y además que el router no tomara como elegible esa ruta pues no confiará en su origen, es más este no la tomara en cuenta para su tabla de enrutamiento.

La forma de ver la distancia administrativa es mediante el comando show ip route.

```
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 not set

10.0.0.0/24 is subnetted, 1 subnets

C 10.1.1.0 is directly connected, Serial0/0/0

186.42.0.0/24 is subnetted, 1 subnets

C 186.42.37.0 is directly connected, Serial0/0/1

R 192.168.0.0/24 [120/1] via 10.1.1.2, 00:00:02, Serial0/0/0

[120/1] via 186.42.37.2, 00:00:05, Serial0/0/1

C 192.168.1.0/24 is directly connected, FastEthernet0/0

R 192.168.10.0/24 [120/1] via 10.1.1.2, 00:00:02, Serial0/0/0

R 192.168.20.0/24 [120/1] via 186.42.37.2, 00:00:05, Serial0/0/1

(Systems, 2012)

Como se puede apreciar en el comando anteriormente mostrado esta es una topología con RIP v2 que se tiene como topología de prueba se puede verificar en lo resaltado

anteriormente en amarillo que se tiene una distancia administrativa de 120 y la métrica en todos los casos es 1 por lo cual se puede determinar que se aplicara el balanceo de cargas para determinar la ruta a escoger por el router.

Viéndolo con otro comando que se llama show ip protocols por tratarse de RIP v2 se van a publicar las redes que mantiene cada router en este caso es una topología en forma triangular lo cual indica que cada router tendrá tres redes o administrará al menos tres redes de las cuales una es red interna y las otras dos son redes vecinas que pertenecen a un router externo esto pues se trabaja con RIP que como se mencionó anteriormente es un protocolo que se utiliza para redes extensas pues se volvería demasiado pesada su tabla de enrutamiento. Se verá de la siguiente manera.

```
Router#show ip protocols

Routing Protocol is "rip"

Sending updates every 30 seconds, next due in 25 seconds

Invalid after 180 seconds, hold down 180, flushed after 240

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Redistributing: rip

Default version control: send version 2, receive 2
```

Interface	Send	Recv	Triggered RIP	Key-chain
Serial0/0/0	2	2		
Serial0/0/1	2	2		

Automatic network summarization is not in effect

Maximum path: 4

Routing for Networks:

10.0.0.0

186.42.0.0

192.168.1.0

Passive Interface(s):

FastEthernet0/0

Routing Information Sources:

Gateway	Distance	Last Update
10.1.1.2	120	00:00:20
186.42.37.2	120	00:00:00

Distance: (default is 120)

(Systems, 2012)

En amarillo se encuentran las redes mencionadas anteriormente y en azul se encuentra las redes de routers vecinos y la distancia administrativa. **(Ver figura 1)**

4.7.2 Redes conectadas directamente

Las redes conectadas directamente son reconocidas por el router en el mismo instante en que se da la configuración ip a la interfaz claro que para esto la interfaz debe de estar subida y lista para trabajar, cabe recalcar que la distancia administrativa de las redes conectadas directamente es 0, como se mencionó anteriormente mientras menor sea la distancia administrativa más confiable la ruta es por lo tanto es más elegible al momento de tomar la decisión por el router. Al ser la distancia administrativa 0 no se muestra al momento de realizar un show ip route.

```
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 not set

10.0.0.0/24 is subnetted, 1 subnets

C 10.1.1.0 is directly connected, Serial0/0/0

186.42.0.0/24 is subnetted, 1 subnets

C 186.42.37.0 is directly connected, Serial0/0/1

R 192.168.0.0/24 [120/1] via 10.1.1.2, 00:00:12, Serial0/0/0

[120/1] via 186.42.37.2, 00:00:00, Serial0/0/1

C 192.168.1.0/24 is directly connected, FastEthernet0/0

R 192.168.10.0/24 [120/1] via 10.1.1.2, 00:00:12, Serial0/0/0

R 192.168.20.0/24 [120/1] via 186.42.37.2, 00:00:00, Serial0/0/1

(Systems, 2012)

Como se puede observar en lo resaltado anteriormente se tiene que no se ve la distancia administrativa es porque a este router están directamente conectada esa red por lo tanto no se ve la necesidad de mostrar una distancia administrativa de cero.

Capítulo 5

5 Protocolos Vector distancia

5.1 Introducción del protocolo.

Como se ha mencionado para redes extensas es más fácil administrar con protocolos de enrutamiento dinámico, ya que si sufre alguna modificación o problema las constantes actualizaciones del protocolo ayudar a verificar la convergencia en la red. Para los protocolos que se rigen al vector distancia se estudiará: RIP, IGRP y EIGRP.

Para entender cómo trabajan estos protocolos, interpretaremos su nombre: “vector” es porque necesita de una dirección, en este caso sería el equipo próximo o vecino al cual se van a enviar los paquetes y llegar a la red destino, por otro lado el término “distancia” ya que se cuenta los saltos es decir cuán lejos está el destino. **(Ver figura 1)**

Para aplicar estos protocolos hay que tener en cuenta:

1. Tamaño de la red a implementar
2. Que los equipos a utilizar sean compatibles con los protocolos
3. El conocimiento que tenga el administrador para el uso de los protocolos y las topologías.

5.1.1 Funcionamiento:

Como se está analizando, los protocolos por vector distancia difunde la información de su tabla de enrutamiento a través de broadcast cada cierto tiempo así la topología de la red no haya cambiado (información redundante) se dan análisis de capa 3, hay que tener en cuenta que esto consume ancho de banda, procesamiento y si se envían al mismo tiempo se podría crear colisiones. Los routers que usan el protocolo solo comparten la información de sus redes locales y la de sus vecinos, lo que quiere decir que no se tiene conocimiento de toda la red, sino de vías de cómo llegar a la red destino.

5.1.2 Características

Los protocolos de enrutamiento deben tener las siguientes características principales:

Convergencia: se trata del tiempo y capacidad en que los elementos alcanzan o tienen intercambio de información del enrutamiento de la red para fortalecer el correcto desempeño y es proporcional al tamaño de la red, en caso de que no haya convergencia o los tiempos sean muy bajos se corre el riesgo que se presente Routing loop por inconsistencias en la tabla de enrutamiento.

Los tiempos depende de:

- La velocidad en propagar cualquier cambio en la red a los dispositivos vecinos

- Tiempo para detectar las mejores rutas.

5.1.3 Escalabilidad

Es la propiedad o habilidad en que los protocolos de enrutamientos puedan adaptarse a un crecimiento o cambio de la red sin afectar la fluidez de los servicios, teniendo en cuenta que redes más grandes se usaran tiempos elevados de convergencia.

Subnetting: Hay que tener en cuenta que los protocolos de enrutamiento pueden ser con clase o sin clase. Los protocolos con clases permiten el uso de VLSM lo cual facilita el resumen, en cambio los protocolos sin clases no incorporan en la información la máscara de subred.

Recursos: Para los requisitos de los protocolos los recursos que se ocupen es un aspecto fundamental para el funcionamiento o agilidad del enrutamiento ya que a mayores procesos, uso de memoria, ancho de banda el hardware debe ser potente para permitir el correcto funcionamiento.

Implementación: Este aspecto depende del administrador de la red y a como se forme la topología de tal manera que la implementación y mantenimiento se ajuste al protocolo a usar.

5.2 Protocolo de información de enrutamiento (RIP)

Hay que tener presente que RIP es un protocolo de IGP que usa el protocolo vector distancia es decir cuantifica los saltos para llegar a su destino y lo establece como métrica, hay que tener presente que el límite de saltos para dicho protocolo es de 15, a partir del 16avo ya se considera una red inalcanzable esto es con el fin de no crear un routing loop. **(Vea figura 2)**

Como todo protocolo RIP tiene sus pros y contras:

5.2.1 Ventajas:

- Acepta varias versiones, así no sea compatible, esto lo hace un protocolo abierto.
- Es uno de los protocolos más fáciles de configurar
- y como un punto sobresaliente es compatible con la mayoría de equipos en el mercado
- Envía actualizaciones cada 30 segundos por broadcast.
- Puede permitiré balanceo de cargas, pero del mismo costo.

5.2.2 Desventajas:

- Solo toma como referencia los saltos hacia la red de destino, sin tener en cuenta el coste de la ruta.
- En el caso que supere los 15 saltos, el destino se lo considera como inalcanzable.
- Y no tiene el conocimiento para resolver problemas de enrutamiento.

5.2.3 Funcionamiento:

1. Una vez iniciado el protocolo, este envía un mensaje a los routers vecinos, solicitando las tablas de enrutamiento
2. Los equipos vecinos entregan la copia de sus tablas de enrutamiento.
3. Cuando el protocolo se encuentre en modo activo actualizaciones cada 30 segundos con su tabla de enrutamiento a los equipos vecinos por broadcast[32].
4. Cualquier cambio en la métrica se procederá a difundir por broadcast.
5. Los equipos que reciban las respuestas validará o actualizará las tablas de enrutamiento según la información receptada.

[32] Es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea.

5.2.4 Actualizaciones en RIP

El protocolo de enrutamiento RIP tiene como principal características difundir los cambios de red cada 30 segundos, en este lapso se propaga la información así no haya cambios, enviando la tabla de enrutamiento completa en forma de broadcast. Se debe tener presente que si se propagan varias actualizaciones al mismo tiempo se pueden crear colisiones, creando así delays y perjudicando el desempeño de la red. **(Vea figura 3)**.

Esta información puede indicar algún tipo de cambio en la tabla de enrutamiento ya sea por alguna falla o introducción de un enlace, falla de un dispositivo (router) o se detecta alguna mejor ruta (menos saltos).

5.2.4.1 Updates disparados

Estas actualizaciones se dan cuando se detecta alguna falla en el enrutamiento, el router detecta el problema y envía un update sin importar si el tiempo de actualización (30 segundos) haya vencido a los equipos vecinos. Esto nos permite tener una rapidez en la convergencia de la red. Estos updates se dan cuando:

- Se crea una nueva ruta.
- Se declara una ruta inalcanzable.
- Problema en alguna interfaz.

5.2.4.2 Temporizadores.

Existen temporizadores suplementarios que usa RIP y pueden ser verificados con los protocolos antes mencionados como show ip route y show ip protocols.

De invalidez: Este valor se resetea cada vez que llega un mensaje de actualización, por estándar es de 180 segundos que es el tiempo que la ruta se determina como invalida (almacenada en la tabla de enrutamiento) y su métrica se hará de 16.

De Purga: es el tiempo que tomara el Router para eliminar una ruta declarada inválida, el tiempo es de 240 segundos (60 más a los de invalidez).

De espera: Este tiempo de 180 segundos sirve para estabilizar el enrutamiento en RIP, ya que si el router detecta una red como inalcanzable, esperara 180 segundos para poder nuevamente actualizaciones, así evitando los bucles y rutas erróneas al realizar un cambio o falla en la red.

5.3 IGRP (protocolo de enrutamiento de gateway interior)

Cabe indicar que este protocolo es patentado y desarrollado por CISCO, también de vector distancia pero aquí ya se incluye algo del coste de la ruta (ancho de banda, el retado y la carga del enlace). Este protocolo no acepta subnetting es decir es protocolo con clase.

De igual manera que RIP, IGRP envía actualizaciones cada 90 segundos.

5.4 EIGRP (protocolo de enrutamiento de gateway interior mejorado)

EIGRP se considera como un protocolo avanzado ya que tiene características de protocolos de estado de enlace, puede balancear cargas y a diferencia de RIP e IGRP no envía actualizaciones cada cierto tiempo, sino que solamente cuando existe algún tipo de cambio en la topología, mejorando así el procesamiento y la convergencia, además que es mucho más fácil que configurar que OSPF y como aspecto principal, permite el uso de VLSM para así lograr resumen de rutas, hasta de manera manual. Usa menor ancho de banda que RIP. **(Ver figura 4)**

5.4.1 Actualizaciones

La mejora de este protocolo de enrutamiento se da en las actualizaciones, ya que EIGRP envía actualizaciones solo cuando ha existido un cambio en la topología y envía la información no de toda la tabla d enrutamiento sino solo de la red que ha sufrido el cambio, teniendo en cuenta que las actualizaciones llegaran solo a los equipos que necesiten de esta información evitando inundar el canal de comunicación con actualizaciones redundantes.

Puntos a rescatar:

1. Las actualizaciones no se dan en un tiempo específico, es decir no es de manera regular.

2. Son limitadas, ya que solo se envía la información a los routers que necesiten de la misma.
3. Son parciales, solo se da cuando hay un cambio en la red.

5.4.2 BUCLES (routing loops)

Es cuando se envía constantemente los paquetes entre routers creyendo que el otro router sabrá el camino para llegar a la red destino por tener en la tabla de enrutamiento la ruta como válida, sin llegar al objetivo ya sea porque es inalcanzable y formando un loop infinito. **(Vea figura 5)**

Se produce por las siguientes razones:

- Mala Configuración de rutas estáticas o de rutas de descarte.
- Incongruencia en los datos de la tabla de enrutamiento.

Consecuencias:

- Perdida de paquetes
- Menor rendimiento de la red
- Uso inútil de procesos del CPU del router
- Perdida de los updates de enrutamiento
- Afectación a la convergencia de la red
- Consumo de ancho de banda

Soluciones:

1. *Definir una métrica máxima:* En este método se define la cantidad de saltos que dará el paquete antes de ser desechado como por ejemplo en RIP al salto 16 ya se considera una ruta inalcanzable y se desecha el paquete. En el protocolo IP esto se define como el TTL. **(Ver figura 6)**
2. *Horizonte dividido:* Este método indica que no tiene sentido publicar una red por la interfaz que se acaba de recibir la actualización. **(Ver figura 7)**
3. *Envenenamiento de ruta o en reversa:* En este método cuando hay una falla en un enlace, se procede a poner la métrica de 16 (ruta inalcanzable) y propaga con un update para que los demás routers interpreten que la ruta ya no está disponible. Esto da mayor eficacia a la convergencia de la red. **(Ver figura 8).**
4. *Horizonte dividido con envenenamiento en reversa:* Así como el proceso que se en el horizonte dividió, se complementa que a la información de la red que se obtiene en una interfaz se la establece como inalcanzable, esto se hace con el fin de que no haya updates inapropiados.
5. *Temporizador de espera* **(Ver figura 9).**
6. *Updates disparados*

5.5 Protocolo IP (TTL)

Este campo de 1 byte que funciona básicamente como un contador, el cual se va a ir decreciendo uno en uno cada vez que se envía un datagrama IP o pasa por un router,

para limitar una cantidad de enlaces si el campo pasa a valor 0 y no llega el paquete al destino deseado, es descartado. Se usa para eliminar el bucle de enrutamiento y así el paquete no esté circulando en la red de forma infinita. **(Vea figura 10)**

El TTL es independiente de las cantidad de saltos que poseen los protocolos de enrutamiento para determinarlo inalcanzable, como por ejemplo RIP (16 saltos)

Como se ha indicado TTL es un contador de enlaces (interfaces) y no como comúnmente cae en el error de que este campo cuenta los saltos (cantidad de routers).

Capítulo 6

6. Protocolo de información de enrutamiento (RIP)

6.1 Introducción

Uno de los primeros protocolos de enrutamiento dinámico en utilizarse fue RIP (Routing Information Protocol) o en español Protocolo de Información de enrutamiento, este protocolo es ampliamente utilizado incluso en nuestros tiempos por su confiabilidad y alta compatibilidad con el resto de protocolos de enrutamiento ya que la gran mayoría de ellos se basaron en RIP para su desarrollo.

La compresión completa de RIP es importante porque aún se utiliza y es la base para comprender los protocolos de enrutamiento dinámicos que se vienen en capítulos posteriores.

6.2 RIP v1: protocolo de enrutamiento con clase por vector distancia

6.2.1 Información Útil

RIP es un protocolo de enrutamiento dinámico por vector distancia bien antiguo. Si una de las falencias de RIP es que carece de la sofisticación de sus hermanos protocolos de enrutamiento más avanzados, uno de sus fuertes es su utilización en forma continua en redes pequeñas por su facilidad de configuración y su operación.

RIP no es un protocolo en extinción, se está planeando y ya existe al momento una nueva versión que trabaja con IPv6[33] una dirección hexagesimal que se llamará RIP NG (next generation) o en español próxima Generación.

Como dato Histórico se tiene la base de RIP en un protocolo desarrollado por XEROX Network System que se llama GWINFO (Gateway information) información de puerto de enlace en español antes de llamarse RIP este protocolo se llamó RFC 1058, realizado por Charles Hedrick en 1988 el cual hizo publicación de las mejoras de este protocolo . Desde estos puntos se dio mejoras a RIP hasta que se creó RIP v2 1994 y se mejoró con RIP NG que se publica en 1997.

[33] Está destinada a sustituir al actual estándar IPv4. Las direcciones IPv6 se escriben como ocho grupos de cuatro dígitos hexadecimales o, lo que es lo mismo, 16 bytes u octetos.

6.2.2 Formato de mensaje y características de RIP v1

6.2.2.1 Características

RIP posee las siguientes características clave

- RIP es un protocolo de enrutamiento de vector distancia.
- RIP utiliza un conteo de saltos como métrica única para la decisión al momento de escoger una ruta.
- Las rutas con saltos mayores a 15 son inalcanzables.
- Se transmiten actualizaciones cada 30 segundos.

6.2.2.2 Formato de mensaje de RIP

Encabezado:

Se especifican 3 campos en el encabezado de cuatro bytes en el campo comando se especifica el tipo de mensaje, el campo versión tiene como dice su nombre la versión de RIP en este caso es el número 1 y el tercer campo debe de ser cero porque este encabezado ofrece espacio para una futura expansión del protocolo. **(Ver figura 1)**

Entrada de la ruta:

La parte de la entrada de la ruta se divide en tres campos. Uno para el identificador de familias de direcciones (el cual se establece con 2 a menos de que el router haga la solicitud de la tabla de enrutamiento completa en cuyo caso se establece el cero), dirección IP y métrica. Una actualización de RIP puede tener hasta 25 entradas de ruta. El MTU[34] del datagrama se establece en 512 bytes sin incluir encabezados IP o UDP[35].

Comando	1 para solicitud 2 para respuestas
Versión	1 para RIP v1 y 2 para RIP v2
Identificador de familias de direcciones	2 para IP a menos que se realice la solicitud de una tabla de enrutamiento completa en cuyo caso es 0
Dirección IP	La dirección de ruta de destino esta puede ser red, subred o algún host dentro de la red
Métrica	Conteo de saltos no mayor a 15 el router que realiza el envío aumenta la métrica verificando el conteo de saltos.

[34] "Maximum Transfer Unit",Una unidad de transmisión máxima es el mayor paquete o cuadro, definido en octetos (bytes de ocho bits), que puede ser enviado en una red de paquetes.
[35] "User Datagram Protocol", Protocolo de red para la transmisión de datos que no requieren la confirmación del destinatario de los datos enviados.

6.2.3 Funcionamiento de RIP

RIP utiliza dos tiempos de mensajes básicos mensaje de solicitud y mensaje de respuesta. Cada interfaz configurada con RIP pide a sus redes o routers vecinos que envíen su tabla enrutamiento completas y este mensaje es respondido por todos y cada uno de los routers que se encuentren dentro de la red, siempre y cuando estos se encuentren en compatibilidad con RIP, el router evalúa cada una de las rutas si la ruta ya existe en su tabla de enrutamiento la reemplaza para mantener esta actualizada siempre y cuando esta ruta tenga menor número de saltos. El router de inicio reenvía a todos los routers de la red su tabla de enrutamiento para que los equipos que se encuentran Utilizando RIP como vecinos actualicen sus rutas.

Clase de direcciones IP y enrutamiento con clase

Anteriormente se dio a conocer que existen varias clases de direcciones IP para lo que es enrutamiento con clase se dio a conocer que se tienen 3 clases de IP clase A , Clase B y Clase C para IPv4 que son direcciones ip de 4 octetos cada octeto de 8 bits estos octetos pueden ser de red o de host . Este conocimiento se afianzará en el capítulo 6 cuando se vea los fundamentos de VLSM y se haga un repaso de lo que es matemático de subneteo.

6.2.4 Distancia administrativa

En el Capítulo 4 de esta tesis se mencionó que la distancia administrativa es la confiabilidad de el origen de una ruta para RIP la distancia administrativa siempre va a ser de 120 en cualquiera de sus versiones.

Esto lo podemos verificar mediante el comando show ip route o show ip protocols como se muestra a continuación

Router#sh 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

10.0.0.0/24 is subnetted, 1 subnets

C 10.1.1.0 is directly connected, Serial0/0/0

186.42.0.0/24 is subnetted, 1 subnets

C 186.42.37.0 is directly connected, FastEthernet0/0

R 192.168.1.0/24 [120/1] via 10.1.1.1, 00:00:21, Serial0/0/0

R 192.168.10.0/24 [120/1] via 10.1.1.1, 00:00:21, Serial0/0/0

[120/1] via 192.168.20.2, 00:00:10, Serial0/0/1

C 192.168.20.0/24 is directly connected, Serial0/0/1

(Systems, 2012)

Haciendo un show ip protocols se puede determinar la versión de RIP que se utiliza y la distancia administrativa como se muestra a continuación

Router#sh ip protocols

Routing Protocol is "rip"

Sending updates every 30 seconds, next due in 13 seconds

Invalid after 180 seconds, hold down 180, flushed after 240

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Redistributing: rip

Default version control: send version 1, receive 1

Interface	Send	Recv	Triggered RIP	Key-chain
Serial0/0/1	1	1		
Serial0/0/0	1	1		

Automatic network summarization is not in effect

Maximum path: 4

Routing for Networks:

192.168.10.0

192.168.20.0

192.168.30.0

Passive Interface(s):

FastEthernet0/0

Routing Information Sources:

Gateway	Distance	Last Update
192.168.20.1	120	00:00:28
192.168.10.1	120	00:00:08

Distance: (default is 120)

(Systems, 2012)

En azul se ve la versión y en amarillo la distancia administrativa.

6.2.5 Configuración básica de RIP v1

6.2.5.1 Configuración

Para simular la configuración de RIP se va a hacer uso de 3 routers cuya topología se va a poner en la figura 2 de este capítulo. **(Ver figura 2)**

Se va a utilizar la siguiente tabla de enrutamiento.

Dispositivo	Interfaz	Direccion IP	mascara de Subred
R1	Fa 0/0	192.168.0.1	255.255.255.0
	Ser 0/0/0	192.168.10.1	255.255.255.0
R2	Fa 0/0	192.168.20.1	255.255.255.0
	Ser 0/0/0	192.168.10.2	255.255.255.0
	Ser 0/0/1	192.168.30.1	255.255.255.0
R3	Fa 0/0	192.168.40.1	255.255.255.0
	Ser 0/0/0	192.168.30.2	255.255.255.0

6.2.5.2 Habilitación de RIP

Para la habilitación de cualquier protocolo de enrutamiento dinámico se hace uso del comando router y este se ingresa en el modo de configuración global

El mismo router nos va a indicar que protocolos de enrutamiento puede utilizar como se muestra a continuación.

```
Router 1(config)# router ?
```

bgp Border Gateway Protocol (BGP)

eigrp Enhanced Interior Gateway Routing Protocol (EIGRP)

ospf Open Shortest Path First (OSPF)

Rip Routing Information Protocol (RIP)

(Systems, 2012)

Por ejemplo según lo mostrado anteriormente nuestro router el cisco 1841 es compatible con BGP, EIRGP, OSPF y RIP.

Para el desarrollo de este capítulo se va a hacer uso del comando router rip para poder llamar al protocolo RIP en cualquiera de sus versiones.

En caso de no querer que se active este protocolo es necesario solamente poner la palabra “no” en el comando para eliminar el uso de este protocolo quedaría **no router rip.**

6.2.5.3 Especificación de redes

Cuando se ingresa al modo de configuración de RIP se tiene que agregar las redes adyacentes o vecinas haciendo uso del comando **network** de esta forma se agregan y se publican las redes que tiene el router internamente y las redes que este tiene como vecinas cada 30 segundos.

Por ser RIP un protocolo de enrutamiento dinámico con clase al momento que se ingrese una dirección de subred este la convertirá automáticamente a su red original según la clase que esta ip tenga como por ejemplo si se pone una 10.0.0.1/24 esta es una ip clase A, pero esta subneteada para ser tratada como una C, pero el router reconocerá a la red como clase A es decir 10.0.0.0.

Por ejemplo si se maneja la topología mostrada en el figura 5b, la configuración para el router 1 seria:

```
Router 1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router 1(config)#router rip
Router 1(config-router)#version 1
Router 1(config-router)#network 192.168.0.1
Router 1(config-router)#network 192.168.10.1
```

(Systems, 2012)

Como se puede ver en lo marcado con amarillo se ponen las ip de las redes que se tiene como vecinas, el router reconoce las redes sin subneteo y esto lo podemos ver mediante el uso del comando show ip protocols

```
Router 1#sh ip proto
```

Routing Protocol is "rip"

Sending updates every 30 seconds, next due in 14 seconds

Invalid after 180 seconds, hold down 180, flushed after 240

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Redistributing: rip

Default version control: send version 1, receive 1

Interface	Send	Recv	Triggered RIP	Key-chain
FastEthernet0/0	1	1		
Serial0/0/0	1	1		

Automatic network summarization is in effect

Maximum path: 4

Routing for Networks:

192.168.0.0

192.168.10.0

Passive Interface(s):

Routing Information Sources:

Gateway Distance Last Update

Distance: (default is 120)

(Systems, 2012)

Para tener convergencia en toda la red debemos repetir este proceso con router 2 y router 3 con las redes vecinas de cada uno de ellos.

Router 2:

Router 2(config)#router rip

Router 2(config-router)#version 1

Router 2(config-router)#network 192.168.20.0

Router 2(config-router)#network 192.168.10.0

Router 2(config-router)#network 192.168.30.0

Router 2(config-router)#end

Router 3:

Router 3(config)#router rip

Router 3(config-router)#version 1

Router 3(config-router)#network 192.168.40.0

Router 3(config-router)#network 192.168.30.0

Router 3(config-router)#end

(Systems, 2012)

Para comprobar esto lo mejor que se puede hacer es verificar mediante el comando show ip protocols, y el show ip route donde se puede determinar las posibles fallas en configuración

Router 1:

Router 1#sh ip pro

Routing Protocol is "rip"

Sending updates every 30 seconds, next due in 16 seconds

Invalid after 180 seconds, hold down 180, flushed after 240

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Redistributing: rip

Default version control: send version 1, receive 1

Interface	Send	Recv	Triggered RIP	Key-chain
Serial0/0/0	1	1		
FastEthernet0/0	1	1		

Automatic network summarization is in effect

Maximum path: 4

Routing for Networks:

192.168.1.0

192.168.10.0

Passive Interface(s):

Routing Information Sources:

Gateway	Distance	Last Update
192.168.10.2	120	00:00:21

Distance: (default is 120)

Router 2:

Router 2#sh ip protocols

Routing Protocol is "rip"

Sending updates every 30 seconds, next due in 1 seconds

Invalid after 180 seconds, hold down 180, flushed after 240

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Redistributing: rip

Default version control: send version 1, receive 1

Interface	Send	Recv	Triggered RIP	Key-chain
FastEthernet0/0	1	1		
Serial0/0/1	1	1		
Serial0/0/0	1	1		

Automatic network summarization is in effect

Maximum path: 4

Routing for Networks:

192.168.10.0

192.168.20.0

192.168.30.0

Passive Interface(s):

Routing Information Sources:

Gateway	Distance	Last Update
192.168.10.1	120	00:00:19
192.168.30.2	120	00:00:01

Distance: (default is 120)

Router 3:

Router 3#sh ip protocols

Routing Protocol is "rip"

Sending updates every 30 seconds, next due in 2 seconds

Invalid after 180 seconds, hold down 180, flushed after 240

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Redistributing: rip

Default version control: send version 1, receive 1

Interface	Send	Recv	Triggered RIP	Key-chain
FastEthernet0/0	1	1		
Serial0/0/0	1	1		

Automatic network summarization is in effect

Maximum path: 4

Routing for Networks:

192.168.30.0

192.168.40.0

Passive Interface(s):

Routing Information Sources:

Gateway	Distance	Last Update
192.168.30.1	120	00:00:21

Distance: (default is 120)

(Systems, 2012)

Se pueden ver también las rutas creadas por RIP como se muestra a continuación

Para router 1:

```
Router 1#sh 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

C 192.168.1.0/24 is directly connected, FastEthernet0/0

C 192.168.10.0/24 is directly connected, Serial0/0/0

R 192.168.20.0/24 [120/1] via 192.168.10.2, 00:00:04, Serial0/0/0

R 192.168.30.0/24 [120/1] via 192.168.10.2, 00:00:04, Serial0/0/0

R 192.168.40.0/24 [120/2] via 192.168.10.2, 00:00:04, Serial0/0/0

Para router 2

Router 2#sh 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

R 192.168.1.0/24 [120/1] via 192.168.10.1, 00:00:18, Serial0/0/0

C 192.168.10.0/24 is directly connected, Serial0/0/0

C 192.168.20.0/24 is directly connected, FastEthernet0/0

C 192.168.30.0/24 is directly connected, Serial0/0/1

R 192.168.40.0/24 [120/1] via 192.168.30.2, 00:00:20, Serial0/0/1

Para router 3:

Router 3#sh 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

R 192.168.1.0/24 [120/2] via 192.168.30.1, 00:00:03, Serial0/0/0

R 192.168.10.0/24 [120/1] via 192.168.30.1, 00:00:03, Serial0/0/0

R 192.168.20.0/24 [120/1] via 192.168.30.1, 00:00:03, Serial0/0/0

C 192.168.30.0/24 is directly connected, Serial0/0/0

C 192.168.40.0/24 is directly connected, FastEthernet0/0

(Systems, 2012)

6.3 Interfaces pasivas

Según lo anteriormente mencionado en el ejercicio de la topología del figura 5b se puede determinar que la interfaz fa 0/0 de cada una de los routers en esa topología no son interfaces que necesiten actualizaciones de RIP pues no son interfaces de WAN.

Para poder eliminar este tráfico que no es necesario que se genere se crean las interfaces pasivas se podría también eliminar este tráfico quitando la red a la actualización del RIP pero esto no es del todo correcto porque qué pasaría si la ip cambia se necesitaría tener en cuenta que red maneja la LAN del router para esto se presenta la solución mediante el comando **passive-interface** de esta manera

ponemos la interfaz como interfaz pasiva y no se envía actualización de RIP hacia ella. La aplicación de esto se ve al momento de hacer un show ip protocols.

Sintaxis de configuración:

```
Router 1(config)#router rip
Router 1(config-router)#passive-in
Router 1(config-router)#passive-interface fa 0/0
```

Verificación:

```
Router 1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 15 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive 1
  Interface          Send  Recv  Triggered RIP  Key-chain
```

Serial0/0/0 1 1

Automatic network summarization is in effect

Maximum path: 4

Routing for Networks:

192.168.1.0

192.168.10.0

Passive Interface(s):

FastEthernet0/0

Routing Information Sources:

Gateway Distance Last Update

192.168.10.2 120 00:00:07

Distance: (default is 120)

(Systems, 2012)

6.4 Actualizaciones de RIP

6.4.1 Proceso de actualizaciones de RIP

Reglas:

- Si una actualización de enrutamiento y la interfaz que la recibe pertenecen a la misma red principal, la máscara de subred de la interfaz se aplica a la red de actualización de enrutamiento.
- Si una actualización de enrutamiento y la interfaz pertenecen a diferentes redes principales, la máscara de subred con clase de la red se aplica a la red de actualización del enrutamiento.

6.4.2 Ventajas y desventajas del resumen automático

6.4.2.1 Ventaja

- Se envían y reciben actualizaciones de enrutamiento menores, que utilizan menor ancho de banda para las actualizaciones de enrutamiento.

6.4.2.2 Desventaja

- Los protocolos de enrutamiento con clase no incluyen la máscara de subred en las actualizaciones de enrutamiento. Las redes se resumen

automáticamente a través de los bordes de redes principales, ya que el router receptor no puede determinar la máscara de la ruta. Esto se debe a que la interfaz receptora puede tener una máscara diferente de las rutas divididas en subredes

Capítulo 7

7 RIP v2

7.1 Introducción

RIP v2 llamado también RFC 1723, este protocolo es el primer protocolo de enrutamiento sin clase que se discute dentro del desarrollo de esta tesis, este protocolo pierde popularidad cuando surge el EIGRP , el OSPF e IS-IS , que ofrecen más funciones de enrutamiento que RIP v2.

Si bien RIP v2 carece de capacidades del el resto de protocolos de enrutamiento sin clase lo que lo hace popular es la gran compatibilidad que se tiene sobre todo con sistemas en base UNIX[36].

Las mejoras de RIP v2 con respecto a RIP v1 son las siguientes:

- Direcciones de siguiente salto incluidas en las actualizaciones de enrutamiento.
- Uso de direcciones multicast[37] al enviar actualizaciones.
- Opción de autenticación disponible.

[36] Sistema operativo creado por AT&T a mediados de los 70.
[37] Comunicación entre un solo emisor y múltiples receptores en una red.

7.2 Limitaciones de RIP V1

Rutas estáticas o interfaces nulas.

Una de las limitaciones que tiene RIP v1 rutas estáticas nulas muchas veces se utilizan estas rutas para poder representar rutas hacia superredes dentro de una misma red es decir una ruta que contenga un paquete de rutas de esta forma se compacta la tabla de enrutamiento y se optimiza el espacio y la saturación de los enlaces

La forma de configurar esto es mediante el comando

```
R2(config)#ip route 192.168.0.0 255.255.0.0 Null0
```

Redistribución de ruta.

Esto significa tomar las rutas de una fuente de enrutamiento y reenviarlas a otra fuente de enrutamiento el comando es “redistribute static”

Quedaría de la siguiente manera

```
R2(configrouter)# redistribute static
```

7.2.1 Incompatibilidad de RIP v1 con VLSM

Debido a que RIP v1 es un enrutamiento con clase, no envía la máscara de subred, esto hace que al rato de aplicar subnetting o VLSM, se cause un problema pues no todas las divisiones de grupos de IPs que se hacen en VLSM se pueden clasificar o poner con enrutamiento por clases de ip, lo cual causa un problema pues esto hace que lograr una mejor distribución de la red sea imposible.

7.3 Configuración de RIP v2

Al igual que RIP v1 primero se define mediante el comando router RIP que se va a usar el protocolo de enrutamiento RIP, una vez realizado esto se procede a establecerla versión de RIP que se va a utilizar en este caso RIP v2, una vez ejecutado el comando anterior se ejecuta el comando versión para establecer la versión de RIP que se va a utilizar.

```
Router(config)#router rip
Router(config-router)#version 2
```

(Systems, 2012)

De esta forma se habilita el protocolo de enrutamiento RIP v2 mediante un show ip protocols se confirma que este operativo

Aquí se tiene un ejemplo de lo explicado anteriormente con RIP version 2 en ejecución

```
Router#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 26 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send  Recv  Triggered RIP  Key-chain
  Serial0/0/0        2     2
  FastEthernet0/0    2     2
  Serial0/0/1        2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
     10.0.0.0
```

192.168.1.0

192.168.20.0

Passive Interface(s):

Routing Information Sources:

Gateway	Distance	Last Update
10.1.1.2	120	00:00:04

Distance: (default is 120)

(Systems, 2012)

Como se puede mostrar en la ejecución de este comando se está propagando la tabla de enrutamiento hacia la red indicando todas y cada una de las redes que este router maneja. Se ha armado una topología de apoyo la cual será sustentada en el manual de prácticas adjunto, a la ejecución de esta publicación además de estar adjunto en el consolidado de adjuntos haciendo referencia al figura 1.**(Ver figura 1)**

7.4 Verificación de operatividad y diagnóstico de problemas en RIP v2

Hay muchos motivos por los cuales una topología no puede funcionar la recomendación de esta tesis es seguir las capas del modelo OSI comenzando desde la capa física, verificando fallas del cableado o la interfaz que esté dando problemas, enlace viendo que cada interfaz levante de manera correcta, red verificando la

configuración IP asignada a cada de las interfaces esto se hace con el comando "show ip interface brief" como se muestra a continuación:

```
Router#sh ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.20.1    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
Serial0/0/0            10.1.1.1        YES manual up                    up
Serial0/0/1            192.168.1.1     YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

(Systems, 2012)

Para verificar la operatividad a nivel de red de la topología se pueden realizar pruebas de ping para lograr verificar y comprobar la convergencia de la red se muestra el resultado:

```
PC>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=13ms TTL=254
```

Reply from 192.168.1.2: bytes=32 time=6ms TTL=254

Reply from 192.168.1.2: bytes=32 time=10ms TTL=254

Reply from 192.168.1.2: bytes=32 time=10ms TTL=254

Ping statistics for 192.168.1.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 6ms, Maximum = 13ms, Average = 9ms

Es necesario recordar siempre que para que se tenga convergencia es necesario que todos los routers de la red hablen el mismo idioma, es decir que tienen que estar configurados dentro del mismo protocolo de enrutamiento en este caso RIP por tratarse de este protocolo es necesario que se verifique también que todos los equipos se encuentren en la misma version de RIP recordando que si no es así se toman IPs con clase y no se toma en cuenta el subneteo de la red. Esto se verifica como se demostró anteriormente mediante el comando **show ip protocols** se muestra a continuación

Router#show ip protocols

Routing Protocol is "rip"

Sending updates every 30 seconds, next due in 24 seconds

Invalid after 180 seconds, hold down 180, flushed after 240

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Redistributing: rip

Default version control: send version 2, receive 2

Interface	Send	Recv	Triggered RIP	Key-chain
Serial0/0/0	2	2		
FastEthernet0/0	2	2		
Serial0/0/1	2	2		

Automatic network summarization is in effect

Maximum path: 4

Routing for Networks:

10.0.0.0

192.168.1.0

192.168.20.0

Passive Interface(s):

Routing Information Sources:

Gateway	Distance	Last Update
10.1.1.2	120	00:00:05
192.168.1.2	120	00:00:07

Distance: (default is 120)

(Systems, 2012)

En la primera marcación se puede ver que se está ejecutando el protocolo RIP, en la segunda marcación se ve la versión y en la tercera se ve la distancia administrativa la cual para RIP en cualquiera de sus versiones siempre va a ser 120.

Capítulo 8

8 Tabla de enrutamiento.

8.1 Introducción.

Como se ha mencionado en capítulos anteriores la tabla de enrutamiento no es otra cosa que un compilado o registros de rutas almacenada en el router para determinar que salto o camino el paquete debe tomar como mejor opción, en la misma que se puede observar si la ruta está conectada directamente a la interfaz del router o es aprendida por un protocolo de enrutamiento teniendo como concepto que todo esto se da en la capa 3 del modelo OSI, no importa de dónde provenga la ruta, esto no

afecta a la tabla de rutas. La información de las tablas de enrutamiento se puede compartir con los nodos aledaños por medio de los protocolos de enrutamiento y así haya conocimiento total de la red diseñada. **(Ver figura 1)**

Cuando se emplea protocolos de enrutamiento estático (redes pequeñas o de fácil diseño), el mantenimiento de la tabla de enrutamiento se lleva de manera manual, es decir que no cambia hasta que el administrador la haga una variación.

La ventaja de registro de direcciones cuando se emplea enrutamiento es que el propio router construye y actualiza la tabla de rutas, siendo así un punto a favor para la convergencia y adaptación de la red cuando hay fallas en enlaces

La estructura de la tabla de rutas se da de manera jerárquica, agilitando de esta manera la búsqueda de mejor opción ruta o envíos. Existen dos niveles para el análisis: 1 y 2

8.2 Rutas nivel 1 y nivel 2

Básicamente las rutas consideradas como de nivel 1, son aquellas que comparando la máscara de subred de la ruta es menor o igual a la de la dirección de red con clase, ejemplo: teniendo una dirección 172.16.1.0/16 se considera que es una red nivel 1 ya que el prefijo de subred para ese tipo B de dirección es de /16. Suelen ser:

1. Rutas por defecto
2. Rutas de superred

3. Rutas de red

Las rutas nivel 1 también son consideradas como rutas finales por tener como información la interfaz de salida o IP de siguiente salto.

No necesariamente debe estar la red conectada de forma directa ya que como se explicó, no importa la procedencia de la dirección.

Para proceder al estudio de las rutas principales y secundarias, vamos a tomar referencia del diseño de red de la figura 2. **(Ver figura 2)**

Si ejecutamos el comando “show ip route” podemos observar que la ruta que va al switch S2, tiene como información 2 direcciones.

```
R2#sho ip rou
Gateway of last resort is not set
    10.0.0.0/24 is subnetted, 1 subnets
C       10.0.3.0 is directly connected, FastEthernet0/0
C    192.168.0.0/24 is directly connected, Serial0/0/1
R2#
```

(Systems, 2012)

Cuando ingresamos la red 10.0.3.0 con sufijo /24, La ruta principal de nivel 1 (color amarillo) es aquella que automáticamente se adiciona en la tabla de enrutamiento la dirección base seguida del sufijo de la dirección de la ruta, en este caso sería la 10.0.0.0/24 pero la diferencia radica en que en esta línea donde se muestra la dirección no hay información de interfaz de salida, ni de IP de siguiente salto. En pocas palabras, es un encabezado que no muestra una interfaz de salida o siguiente salto y nos da paso a una ruta de nivel 2 o secundaria (resaltado de color verde).

En conclusión tenemos que la ruta principal (nivel 1) se crea en la tabla de enrutamiento siempre y cuando la dirección IP tenga una máscara superior a la máscara sin clase y a partir de esto la subred se denomina ruta secundaria (nivel 2). Este ordenamiento o jerarquía sirve para que al momento de enviar paquetes se tome la mejor ruta.

8.2.1 Ruta principal de nivel 1

En la ruta principal encontraremos principalmente la información:

1. Dirección de red con clase
2. La máscara de subred que comparte las rutas de nivel 2 (en el caso que las rutas nivel 2 no tengan por igual la máscara de subred se omitirá dicho campo en la ruta principal),
3. El número de subredes que posee

10.0.0.0 */24* is subnetted, *2 subnets*

1 2 3

8.2.2 Rutas de Nivel 2

Se entiende como la ruta real, también llamadas rutas finales por contar con la interfaz de salida y muestra la siguiente información:

1. Origen de la ruta
2. Dirección de ruta
3. Interfaz de salida

C *10.0.2.0* is directly connected, *Serial0/0/0*

1 2 3

Como se puede evidenciar en la sección de la dirección ya no se muestra la máscara, dicha información la contiene la ruta principal ya que las subredes no tienen VLSM.

En el caso de que las diferentes rutas pertenezcan a una dirección con clase, pero por el uso de subnetting tengan diferentes prefijos de mascara. En la ruta principal aparece a que prefijo pertenece la dirección con clase cosa que no presentaba en los casos que se usaba redes sin VLSM, adicional información de las máscaras se muestra detallada en la ruta secundaria, ejemplo: **(Ver figura 3)**

#show ip route

10.0.0.0/8 is variably subnetted, ***3 subnets, 3 masks***

C ***10.0.2.0/28*** is directly connected, Serial0/0/0

C ***10.0.3.0/30*** is directly connected, Serial0/1/0

C ***10.0.1.0/16*** is directly connected, FastEthernet0/0

(Systems, 2012)

Se puede verificar que en la información destacada que presenta la tabla de enrutamiento es:

1. Dirección IP con clase de la ruta principal.
2. Cantidad de subredes.
3. Cantidad de máscaras variables.
4. Direcciones IP de las rutas secundarias con sus respectivas mascaras variables.

En el ejemplo que estamos analizando, si se realiza enrutamiento por protocolo RIP, vamos a tener fallas en la comunicación y esto se puede determinar viendo la tabla de enrutamiento de los 3 equipos. **(Ver figura 4)**

R1>show ip route

10.0.0.0/24 is subnetted, 3 subnets

C 10.0.1.0 is directly connected, FastEthernet0/0

C 10.0.2.0 is directly connected, Serial0/0/0

R 10.0.3.0 [120/1] via 10.0.2.2, 00:00:21, Serial0/0/0

R 192.168.0.0/24 [120/1] via 10.0.2.2, 00:00:21, Serial0/0/0

R2#show ip route

10.0.0.0/24 is subnetted, 3 subnets

R 10.0.1.0 [120/1] via 10.0.2.1, 00:00:10, Serial0/0/0

C 10.0.2.0 is directly connected, Serial0/0/0

C 10.0.3.0 is directly connected, FastEthernet0/0

C 192.168.0.0/24 is directly connected, Serial0/0/1

R3>show ip route

10.0.0.0/24 is subnetted, 1 subnets

C 10.0.4.0 is directly connected, FastEthernet0/0

C 192.168.0.0/24 is directly connected, Serial0/0/1

(Systems, 2012)

Si estudiamos las rutas en la tabla, se evidencia que no se está registrando convergencia hacia la red 10.0.4.0 desde R1, ni R2. Asimismo R3 no reconoce las rutas conectadas directamente en R1 y R2, esto sucede a que RIP está orientado a direccionamiento sin clase.

8.3 Ruta Preferida

Para la selección de la ruta preferida se realiza un proceso interno, en la cual se escoge la coincidencia más larga, esto consiste en comparar la dirección IP del paquete con la ruta de la tabla, la coincidencia de bit más a la izquierda que tenga mayor similitud a la del paquete se establece como la ruta preferida.

Ejemplo:

192.168.1.5 → 11000000 . 1010100 0 . 00000001 . 0 0000101

192.168.1.0/8	→	**11000000** . 1010100 0 . 00000001 . 0 0000101
192.168.1.0/15	→	**11000000 . 1010100** 0 . 00000001 . 0 0000101
192.168.1.0/25	→	**11000000 . 10101000 . 00000001 . 0** 0000101

En el caso del ejemplo se puede determinar que la ruta preferida para la dirección 192.168.1.5, es 192.168.1.0/25 por tener mayor coincidencia de los bits de la izquierda.

8.4 Comportamiento con clase y sin clase

Hay que tener presente y saber diferencia protocolos de enrutamiento y comportamiento de enrutamiento.

Los protocolos influyen en la forma que se va completando la tabla de enrutamiento y el comportamiento de enrutamiento determina el proceso de búsqueda de la ruta preferida y en el cual se usara los comando IP CLASSLESS (sin clase), NO IP CLASSLESS (con clase).

El comportamiento de enrutamiento no depende de los protocolos, es decir que se puede usar protocolos de enrutamiento sin clase y comportamiento de enrutamiento con clase, eso si no se puede establecer los 2 comportamientos de enrutamiento al mismo tiempo.

Siguiendo con nuestra topología debemos recordar que RIP presenta inconvenientes de comunicación cuando se implementa topologías con redes no contiguas. **(Ver figura 5)**

Como se visualiza en la gráfica entre R2 y R3 hay existe un problema ya que no está reconociendo la procedencia de la red 10.0.4.0/24, En este caso para que establecer convergencia se debe crear una ruta por defecto o también conocida como quad-zero.

La Quad-Zero es una ruta por defecto en caso de que no haya coincidencia en la tabla de enrutamiento y poder enviar el paquete por la interfaz seleccionada en la ruta por defecto.

Show ip Route en R2

10.0.0.0/24 is subnetted, 3 subnets

R 10.0.1.0 [120/1] via 10.0.2.1, 00:00:16, Serial0/0/0

C 10.0.2.0 is directly connected, Serial0/0/0

C 10.0.3.0 is directly connected, FastEthernet0/0

C 192.168.0.0/24 is directly connected, Serial0/0/1

S* 0.0.0.0/0 is directly connected, Serial0/0/1

(Systems, 2012)

Capítulo 9

9 EIGRP

9.1 Introducción a EIGRP

EIGRP debe su nombre a la sigla en inglés Enhanced Interior Gateway Routing Protocol, al igual que RIP este protocolo es un protocolo que funciona por vector distancia, este protocolo es propiedad de Cisco Systems y fue lanzado en 1992 con IOS 9.21. Este protocolo es la evolución de IGRP (interior Gateway Routing Protocol) ambos protocolos por ser propiedad de cisco solo funcionan en routers que mantengan la marca Cisco o que tengan compatibilidad o licencias compradas para hacer uso de estos protocolos.

Las mejoras presentadas con respecto a RIP en cualquiera de sus versiones son las siguientes:

- Cuentan con lo que se llama Reliable Transport Protocol (RTP).
- Actualizaciones limitadas.
- Algoritmo de actualización por difusión.
- Establecimiento de adyacencias.
- Tablas de topología y de vecinos.

El EIGRP proporciona una entrega confiable de paquetes gracias a la utilización del RTP para poder establecer la entrega de paquetes que es un algoritmo que hace una confirmación momentánea de que el paquete llego a su destino este lleva también un registro del estado de sus vecinos verificando cuando estos están activos, cuando no

lo están o incluso cuando están saturados de esta manera se asegura de que al rato de enviarse los paquetes estos lleguen a su destino sin perderse en el camino ni con ningún retraso.

Como actor principal de EIGRP se tiene al algoritmo de actualización por difusión llamado también DUAL, este garantiza que las rutas no tengan bucles repetitivos optimizando el tamaño de la tabla de enrutamiento pues las rutas no se repetirían indefinidamente.

Como RIP v2 EIGRP trabaja con enrutamiento con o sin clase haciendo posible el uso de subnetting para poder hacer una más óptima distribución de la red, dentro de este capítulo se aprenderá a deshabilitar el auto summary, que es la actualización automática a redes que no necesitan este requerimiento, de esta manera se optimizara el tamaño de la tabla de enrutamiento de las actualizaciones que se envían en la red.

9.2 Historia.

Como se mencionó anteriormente EIGRP es la evolución de IGRP ambos protocolos desarrollados por cisco systems en 1985. Estos protocolos fueron creados en vista a las limitaciones que poseía RIP v1 como un protocolo con clase dado a que este tenía una métrica por conteo de saltos y la cantidad máxima de saltos que este soportaba era de 15. Como respuesta a esta limitación de RIP v1 cisco implementa la métrica por asignación de ancho de banda, retraso, confiabilidad y cara de la red, la diferencia entre IGRP y EIGRP es que IGRP en un protocolo de

enrutamiento con clase y por eso hace uso del algoritmo de Bellman-Ford descrito en capítulos anteriores.

9.3 Determinación de la ruta de EIGRP.

Los protocolos de enrutamiento como RIP e IGRP son protocolos por vector distancia, es decir siempre se va a tener cierta cantidad de rutas predeterminadas, de las cuales se tendrá siempre un record o registro.

EIGRP tiene un algoritmo al cual se mencionó en páginas anteriores denominado DUAL el cual mantiene la tabla de enrutamiento de una topología separadas de las de otra, las cuales incluyen siempre el mejor camino o ruta hacia esta y rutas alternas sin bucles en caso de que esta por defecto fallara, de esta forma se asegura el alcance de todas las subredes de una superred.

Si una ruta no está disponible sea porque el enlace no está realizado, alguna ruptura de conductor, alguna falla de la interfaz; DUAL buscara dentro de su tabla de enrutamiento una ruta alterna o una ruta de respaldo válida para interconectar las redes. Si a pesar de esto esta ruta no existiera DUAL realizara un proceso de reconocimiento de la red para buscar la ruta alterna de la red todo esto en cuestión de milisegundos.

DUAL es parte importante de la inteligencia de EIGRP.

EIGRP no utiliza temporizadores de espera, en su lugar rutas que se establecen sin bucles son las utilizadas lo cual se logra a través de lo que se llama cálculo por difusión lo cual se realiza por coordinación entre routers, esto hace que se tenga una convergencia mucho más rápida que otros protocolos de enrutamiento dinámico a los cuales se tenía que esperar que se cumpla el temporizador del protocolo para comenzar a tener convergencia.

9.4 Convergencia.

Generalmente los protocolos de enrutamiento que son de mayor uso como RIP e IGRP , envían actualizaciones cada cierto tiempo , debido a que estos tienen que estar atentos a cualquier cambio que se realice dentro de la red, especialmente RIP e IGRP suelen desarrollar problemas de routing loop debido a esto es decir rutas redundantes en exceso a un mismo punto los cual hace que la tabla de enrutamiento crezca de manera exuberante, haciendo que cada vez esta sea mucho más grande saturando los enlaces por más tiempo y causa mucho más tráfico dentro de la red, además como se mencionó anteriormente estas actualizaciones suelen ser temporizadas a un tiempo seteado por el protocolo , lo cual causa que el tiempo para poder tener convergencia sea mucho más alto. EIGRP no utiliza estos tiempos de espera , en vez de esto , se utiliza un sistema de cálculos de ruta también llamados cálculos por difusión o broadcast, estos se realizan coordinadamente entre routers , de tal manera que la convergencia se logra mucho más rápido, logrando así un tiempo de configuración menor y una operatividad mucho más rápida.

9.5 Formato del mensaje de EIGRP.

Todos los datos de EIGRP son encapsulados en un paquete, este campo es llamado TLV (tiempo / longitud/ valor). Los tipos de TLV que se van a ser de interés de estudio en esta tesis son los parámetros que son generados por EIGRP entre ellos se va a tener Rutas internas de IP y rutas externas de IP. Poco a poco se irá viendo cómo se va desglosando este campo de datos.

Como en todos los paquetes de datos el paquete EIGRP va a tener un encabezado que es donde comienza el paquete. Una vez dicho esto, el encabezado del paquete EIGRP y el TLV se encapsulan en un paquete IP. En el encabezado del paquete ip hay un campo de protocolo el cual va a ser seteado con valor 88 indicando que se trata del protocolo EIGRP. El paquete IP tiene un campo que es llamado destino al cual se va a poner en opción multicast que es envío a varios puntos, para lo cual se establezca la dirección 224.0.0.10. Aclarando de que si EIGRP se encapsula en un paquete Ethernet, la dirección destino será MAC para lo cual se establecerá una dirección MAC multicast que es la 00:5E:00:00:0A.

En la **figura** 1 se puede ver la forma que tiene el mensaje ip donde esta introducido el mensaje EIGRP. **(Ver figura 1)**

El mensaje EIGRP incluye el encabezado. Los puntos más importantes que se analizaran son el código de operación y el campo de número de sistema autónomo.

El comportamiento que identifica a EIGRP es:

- Actualización

- Consulta
- Respuesta
- Saludo

El número de sistema autónomo también llamado AS[38] identifica al proceso de enrutamiento causado por EIGRP. **(Ver figura 2)**

9.6 Cálculo de la métrica de EIGRP.

EIGRP es un protocolo que se basa en la métrica para poder cumplir su misión la cual como cualquier protocolo de enrutamiento siempre va a ser escoger la mejor ruta. EIGRP toma en cuenta los siguientes factores para hacer cálculo de la métrica:

- Ancho de banda
- Retraso o latencia
- Confiabilidad de ruta
- Carga asignada a la ruta

Generalmente se va a hacer recomendación de tratar de hacer este cálculo solo con en ancho de banda y la latencia pues son calculadas así por defecto, solo se recomienda tener en cuenta la confiabilidad de la ruta y la carga cuando se tenga una necesidad explicita de hacerlo.

[38] "Autonomous System", es un conjunto de redes y dispositivos router IP que se encuentran administrados por una sola entidad.

9.6.1 Métrica compuesta.

La fórmula para el cálculo de la métrica compuesto se basa en constantes que se van a establecer dándoles valores mediante un comando que se mostrara posteriormente las constantes se establecerán desde k1 hasta k5, es decir, k1, k2, k3, k4, k5 por defecto los valores de K1 y k3 se establecen en 1 esto deja a k2,k4,k5 en ceros pero estos valores pueden ser cambiados, mediante el siguiente comando:

Router(configrouter)# metric weights tos k1 k2 k3 k4 k5

La métrica compuesta por defecto viene dada por la siguiente formula:

Métrica=(k1*ancho de banda+k3*retraso)

La métrica compuesta completa viene dada por:

Métrica=[k1*ancho de banda+(k2*ancho de banda)/(256-carga)+k3*retraso]*[k5/(confiabiliad+k4]

Los valores asignados a k pueden ser vistos o revisados por el administrador de la red mediante el uso de la sentencia show ip protocols

Router#sh ip protocols

Routing Protocol is "eigrp 1 "

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Default networks flagged in outgoing updates

Default networks accepted from incoming updates

EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0

EIGRP maximum hopcount 100

EIGRP maximum metric variance 1

Redistributing: eigrp 1

Automatic network summarization is in effect

Automatic address summarization:

Maximum path: 4

Routing for Networks:

10.1.1.0/24

192.168.1.0

192.168.10.0

Routing Information Sources:

Gateway Distance Last Update

Distance: internal 90 external 170

(Systems, 2012)

Como se puede observar en lo resaltado con amarillo, se dan valores por defecto desde k1 hasta k5.

9.7 Delimitación del ancho de banda.

La gran mayoría de dispositivos que usan EIGRP, utilizan dicho protocolo para buscar una salida por medio de interfaces seriales es, decir interfaces de salida WAN debido a que EIGPR es un protocolo orientado a la conexión.

Una de las formas de establecer a una ruta como favorita es jugar con el ancho de banda es decir, EIGRP siempre v a escoger por defecto la ruta con mayor ancho de banda pues facilita así una mejor conexión con una liberación de canal más rápida. Esto se puede lograr mediante la sentencia de asignación de ancho de banda, el primer paso es ingresar a la interfaz a la que se va a asignar el ancho de banda deseado, luego mediante el comando bandwidth se establece el ancho de banda deseado par a la interfaz. Se haría de la siguiente manera:

Router(config-if)#int ser 0/0/0

Router(config-if)#bandwidth 64

(Systems, 2012)

De esta forma se asigna el ancho de banda de 64 Kbps[39] a la interfaz serial 0/0/0.

Cabe recalcar que todas las rutas por defecto van a tener siempre asignadas todas el mismo ancho de banda lo cual le da la libertad a EIGRP a escoger cualquier ruta mientras que si se le asigna un ancho de banda debido mayor que las interfaces no asignadas se hace de esa ruta o interfaz la favorita al momento de realizar la propagación de un paquete.

Para deshabilitar la sumarización o habilitar el resumen de rutas innecesarias lo cual como se vio en protocolos de enrutamiento anteriores es para habilitar la velocidad de procesamiento y optimizar la red, se puede hacer unos del comando **no auto-summary.**

9.8 Resumen

EIGRP

Protocolo vector distancia, usa el mismo sistema de métricas que IGRP y que utiliza DUAL (Diffusing Update Algorithm), para crear la base de datos topológica. EIGRP utiliza principios de los protocolos de estado de enlace, x eso es llamado protocolo

[39] Un kilobit por segundo es una unidad de medida que se usa en telecomunicaciones e informática para calcular la velocidad de transferencia de información a través de una red.

hibrido, sería mucho más correcto llamarlo protocolo de vector distancia avanzado. Funciona en IPv4 e IPv6, los fundamentos no cambian.

Utiliza pocos recursos de CPU y memoria.

Cisco define cuatro propiedades principales de EIGRP:

- Protocol – dependent modules: soporta varios tipos de protocolo de capa 3 como IPv4 e IPv6.
- Reliable Transfer Protocol (RTP): Eigrp envía paquetes utilizando protocolos confiables.
- Neighbor discovery and recovery: Eigrp utiliza hellos para identificar a los nuevos routers vecinos y también darse cuenta de la pérdida de los mismos.
- Diffusing Update Algorithm (Dual): es utilizado para identificar las posibles rutas para alcanzar un destino, para luego elegir la mejor; además DUAL selecciona caminos “alternativos” en caso que el principal falle.

FUNCIONAMIENTO DE EIGRP.

Envía actualizaciones confiables, identificando sus paquetes con el protocolo IP nro. 88. Esto significa que el destino debe enviar un acuse de recibo (ACK) al origen, es decir que debe confirmar el recibe de datos.

Los siguientes tipos de paquetes son utilizados:

- Hello: se envían periódicamente usando una dirección multicast (224.0.0.10) para descubrir y mantener relaciones de vecindad.
- Update: anuncian las rutas, se envían de manera de multicast.
- ACK : se envía para confirmar la recepción de un Update.
- Query: se usa como modo de consulta de nuevas rutas cuando el mejor camino se ha perdido. Si el router que envía la consulta no recibe respuesta de algunos de sus vecinos, volverá a enviarla pero ahora en Unicast[40] y así sucesivamente hasta que reciba un reply, hasta un máximo de 16 envíos.
- Reply: es una respuesta a una query, con el camino alternativo o simplemente indicando que no tiene.(R)

Capítulo 10

10 Protocolos de estado de enlace

10.1 Introducción.

El protocolo de estado enlace envía la información de las redes conectadas directamente, creando así una imagen de toda la red y compartiendo la información a los demás dispositivos, si hacemos una analogía el protocolo funciona de la misma forma en que las señales de información en una carretera, es decir el viajero se va

[40] Es el envío de información desde un único emisor a un único receptor.

guiando a través de los carteles sin necesidad de saber que tiene por delante. De la misma manera que los protocolos estudiados anteriormente, la información se mantiene mediante actualizaciones y gastando menor recursos que los protocolos de vector distancia.

La ventaja de este protocolo es que su funcionamiento nos permite llegar a la convergencia de una red grande y su configuración no tiene complejidad.

Los protocolos de estado toman como referencia el costo de la ruta para poder enviar los paquetes de manera más eficiente sin llegar a saturar el enlace, de tal manera que cada dispositivo de la red calcula su costo y se selecciona el de menor costo hacia el router destino. Hay que tener en cuenta que debido a los diversos costos y routers en la red, no siempre la ruta con menor costo es la que tiene menor cantidad de saltos.

10.2 Funcionamiento del protocolo.

Todas la interfaces que se encuentren activas y conectadas directamente en el router pasan a formar parte de la información principal. Es decir los routers van a compartir la información de sus conexiones directas para ir formando el mapa.

Para establecer comunicación con los routers vecinos, se envían paquetes de saludo de las interfaces conectadas directamente.

Se verifica el estado del enlace creando paquetes LSP que adjunta la información del ID del equipo vecino y los costos de la ruta.

Se satura de paquetes LSP a cada router vecino y se va creando una base de datos y así sucesivamente con los demás routers vecinos hasta llegar a todos los routers de la red y tener la base de datos de cada router vecino.

Teniendo una mapa completo de la topología, los routers calculan la mejor ruta para los diferentes destinos, así se tendrá el mejor camino teniendo en cuenta los costos de las rutas.

10.3 Aprendizaje de redes conectadas directamente.

Generalmente cuando se ponen en la misma subred dos interfaces estas tienen comunicación es decir estas se aprenden como rutas conectadas directamente, por lo tanto siempre se van a aprender automáticamente.

Generalmente al momento de hacer un show ip route en cada uno de los routers que están conectados directamente siempre se va a obtener las rutas marcadas con la letra C que son redes conectadas directamente por ejemplo:

```
R1#sh 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

10.0.0.0/30 is subnetted, 1 subnets

C 10.0.0.0 is directly connected, Serial0/0/0

C 192.168.10.0/24 is directly connected, FastEthernet0/0

De esta configuración se puede determinar lo siguiente

R1 está conectado a la red 10.0.0.0 por la seria 0/0/0

R1 está conectado a la red 192.168.10.0/24 por la fast Ethernet 0/0

(Systems, 2012)

10.4 OSPF.

10.4.1 Introducción al OSPF

OSPF es un protocolo de enrutamiento conocido así por sus siglas en ingles Open Shortest Path First es un protocolo de estado de enlace diseñado para ser el reemplazo de RIP , este protocolo por si está orientado a la conexión. RIP tuvo su apogeo en los comienzos del networking y el internet lo cual si se pone a analizar es ya hace algunos años, como se expuso anteriormente RIP tiene muchas limitaciones que lo hacen ideal para redes pequeñas pero cuando se habla de superredes RIP queda corto, recordando que el máximo conteo de saltos que este puede hacer es de máximo quince. OSPF es un protocolo de enrutamiento sin clase lo cual incrementa la capacidad de escalabilidad en la red permitiendo redes subneteadas al momento de publicar las redes vecinas, y por no tener un número máximo de conteo de saltos, OSPF se hace merecedor al título de orientado a conexión. OSPF utiliza como concepto el uso de áreas para lograr escalabilidad del tipo RFC2328 y este define la métrica como un valor al azar llamado costo de esta manera se escoge la mejor ruta a seguir para la entrega de un paquete. Una de las principales ventajas de OSPF contra RIP es la velocidad de la convergencia es decir, cuando se declara una red vecina en la misma área de OSPF esta red automáticamente se vuelve convergente con el resto de redes ya declaradas. (Cisco Systems, 2009)

OSPF da sus orígenes en 1987 gracias a IETF como parte de un proyecto de red académica para intercambiar información.

La primera versión del protocolo se dio en 1989 llamada OSPFv1. Esta se publica en codificación RFC 1131 y fueron establecidas para routers y equipos UNIX. Solo formó como parte de un experimento.

“En 1991 el programador ingeniero Jhon Moy fue el reformador del protocolo OSPF quien hizo ciertas mejoras del protocolo si se verifica el link del referencial se puede notar el memo original de Jon Moy T donde se especifica la codificación del protocolo y las mejoras realizadas a OSPF v1 dejándolo publicado como OSPF v2 en RFC 1247” (Sycamore Networks, Inc.).

Las mejoras del protocolo OSPF se dieron en 1998, siendo la especificación que actualmente se usa RFC 2328 para IPv4. Cabe indicar que pensando en la saturación del espacio de direccionamiento, en 1999 se estableció una versión para IPv6 pero en estándar RFC 2740.

10.4.1.1 Encapsulación OSPF.

Existen 5 tipos de paquetes para el protocolo OSPF en el cual puede ser encapsulado:

El encabezado o header estará incluido en todos los paquetes de este protocolo sin importar el tipo paquete puesto que va a indicar que clase de paquete se recibirá o enviará. Luego estos paquetes de datos son encapsulados en un paquete IP. Para este protocolo se establece por estándar como 89 el campo de protocolo y la dirección de destino del paquete IP se enviará como modo multicast con la siguiente dirección como standard: 224.0.0.5 o en su caso 224.0.0.6. En el caso de tratarse de un paquete

Ethernet esto proceso se realiza en la capa 2 del modelo OSI con un a MAC multicast por defecto de: 01:00:5E:00:00:05 o en su caso 01:00:5E:00:00:06. **(Ver figura 1)**

10.4.1.2 Clases de paquetes.

Los tipos de paquetes de OSPF son también llamados paquetes de estado de enlace LSP. Cada LSP cumple un papel específico en el proceso de OSPF los tipos de paquetes son:

- **Hello o saludo.-** este paquete se utiliza para descubrir adyacencias en otros puntos de la red.
- **DBD.**- Conocido como paquete descriptor de base de datos y Es usado por los routers receptores para ser comparados con la base de estado local.
- **LSR.**- En el caso que se necesite mayor información del DBD, el LSR administra la entrada DBD y se lo realiza mediante una solicitud de enlace LSR.
- **LSU.**- Son respuestas hacia los paquetes LSR y detallan nueva información del enlace, es decir son paquetes de actualización. Se tiene 6 tipos de notificaciones.
- **LSAck.**- cuando se recibe una LSU el router tiene que enviar una confirmación de que se recibió el LSU para esto se utiliza el acuso de recibo o de establecimiento del enlace o LSAck.

(Ver figura 2)

10.4.1.3 Protocolo de saludo.

La función del saludo o hello es de descubrir adyacencias en la topología de la red, pero también tiene otras funciones que se enumeran a continuación:

- Descubrir vecinos
- Publicar parámetros para acordar la forma en la que se establecen los vecinos
- Elegir el router designado (DR) y el router designado de respaldo BDR para redes de acceso múltiple como frame relay y Ethernet.

Los campos más importantes dentro del paquete OSPF son:

- Tipo: si el paquete es : saludo(1) , DD(2), solicitud LS(3), Actualización LS(4), ACK LS(5).
- ID del router: Identificación del router de origen.
- ID del área: Área en el que se origina el paquete.
- Mascara de red: mascara de subred asociada a la emisora
- Intervalo de saludo: cantidad de tiempo generalmente expresada en segundos entre los paquetes de saludo del emisor.
- Prioridad del router: utilizado en la selección de DR o BDR
- Router designado: identificación del DR

- Router designado de respaldo : identificación del BDR
- Lista de vecinos: enumera la cantidad de rutas que existen hacia los vecinos originados por OSPF.

(Ver figura 3)

10.4.1.4 Intervalos muertos y saludo de OSPF.

Para lograr la adyacencia entre vecinos primero se debe determinar los 3 factores:

- **Intervalo de saludo:** La frecuencia con que se realizará el envío de paquetes de saludo por estándar se envían cada 10 segundos en sistemas punto a punto y cada 30 segundos en segmentos multiacceso sin broadcast.
- **El intervalo muerto:** Es el tiempo en el que el router espera un saludo cuando ha sido declarado vecino muerto es decir lleva bastante tiempo sin establecer conexión.
- **Tipo de red.**

10.4.1.5 Selección de DR y BDR.

El DR es el encargado de actualizar todos los routers vecinos, es decir en vez de saturar la red con paquetes de actualización de cada uno de los routers de la red solo lo va a hacer uno al cual se va a llamar router designado (DR), en el caso que el

router designado presente una falla se debe tener BDR o router designado de respaldo.

La asignación de DR y de BDR se hace en redes multiacceso

La elección del DR y BDR se realiza según los siguientes puntos

- DR: Router con la prioridad más alta
- BDR: Router con la segunda prioridad más alta
- Si las prioridades de la interfaz OSPF son iguales, la ID del router mas alta es la que será escogida.

10.4.1.6 Actualizaciones de estado de enlace OSPF.

Las LSU o actualizaciones de estado de enlace, son paquetes que se utilizan para la actualización de OSPF. Esto implica 10 formas diferentes de LSA o notificaciones de estado de enlace. **(Ver figura 4)**

Una LSU puede incluir una o varias LSA y cualquiera de los términos puede utilizarse para hacer la descripción del estado del enlace OSPF ya que las LSA serían un subconjunto propio de las LSU y contienen casi la misma información.

10.4.1.7 Algoritmo de OSPF.

Los routers que se configuran para usar el protocolo de enrutamiento OSPF mantienen una base de datos donde se guardan las LSA recibidas. cuando este recibe las LSA hace uso del algoritmo Shortest path first (SPF) para poder crear su árbol de rutas, este árbol de rutas se utiliza para completar la tabla de enrutamiento ip con las mejores rutas de la red.**(Ver figura 5)**

10.4.1.8 Distancia administrativa.

Como se trató en capítulos anteriores la distancia administrativa es la confiabilidad que se tiene del origen de la ruta. La distancia administrativa por defecto de OSPF es 110.

10.4.1.9 Autenticación.

OSPF se puede configurar para autenticación es decir que solo se comunique con redes externas mediante el uso de un password en sus interfaces, si este password coincide entre interfaces entonces la red es reconocida.

Se aconseja siempre hacer uso de autenticación de la información del enrutamiento transmitida ya que esto aumenta la seguridad dentro de la red, ya que se garantizaría que solo routers que están configurados con esta autenticación se comunicarían entre sí. Cabe recalcar que la autenticación no encripta la tabla de enrutamiento del router.

10.4.2 Configuración básica de OSPF.

Para configurar OSPF se deben de tener claras las siguientes realidades

- OSPF es un enrutamiento sin clase.
- OSPF hace uso en la publicación de redes de una wildcard.
- OSPF es un protocolo que se basa en áreas de enrutamiento.

La configuración básica de OSPF es la tiene el mismo comienzo de cualquier protocolo de enrutamiento anteriormente tratado es decir

1. Se hace mención del protocolo de enrutamiento que se va a usar con si ID.
2. Se declaran las redes vecinas con la wildcard de cada una de ellas.
3. Se declaran las redes que no se quieren publicar en ambos sentidos.

A continuación se enumeran los comandos con una topología básica para configuración de OSPF

Paso #1

```
Router1(config)#router ospf 1
```

Como se puede observar se menciona el protocolo de enrutamiento que se va a utilizar y se le da un id que en este caso se puso el 1

Paso #2

Router1(config-router)#network 192.168.1.0 0.0.0.255 area 0

Router1(config-router)#network 10.1.1.0 0.0.0.3 area 0

Se declaran las redes vecinas es decir para este caso de ejemplo se usó 2 redes lo cual indicaría que se tiene como vecinas a las redes 192.168.1.0/24 y a la red 10.1.1.0/30 recordando que la wildcard es el inverso de la máscara de subred, es decir:

Si se tiene una máscara /30 255.255.255.252 su wildcard sería la cantidad en números que nos hace falta para llegr a 255 en cada octeto es decir quedaría 0.0.0.3

Paso #3

Router1(config-router)#passive-int fa0/0

Este paso es para evitar que se publiquen rutas a puntos innecesarios ya que en la fast Ethernet 0/0 no se tiene ningún router no es necesario publicar tabla de enrutamiento a ese punto. Esto evita la saturación de la red en puntos innecesarios y permite incrementar la velocidad de procesamiento del router.

10.4.3 Establecimiento de una Loopback.

Antes de hacer uso de una configuración loopback[41] se debe de hacer las siguientes preguntas

Que es una loopback?

Una loopback es una interfaz virtual y eta se encuentra en estado up cuando esta es configurada.

¿Para qué sirve?

Una loopback sirve para realizar un procedimiento para entrada directa para servicios o aplicaciones que se den mediante el protocolo TCP/IP que se corren dentro del mismo dispositivo para comunicarse con otros entre sí.

¿Cuál es la ventaja del establecimiento de una loopback?

La ventaja de utilizar una interfaz loopback es que por ser esta una interfaz virtual no depende de cables o dispositivos adyacentes físicos, el uso de esta interfaz trae estabilidad al OSPF.

Para establecer o configurar la loopback esta debe de configurarse en todos los dispositivos de la topología de red, es decir se la tiene que declarar y levantar ojo generalmente es una ip asignada cualquiera que se establece en un router con mascara 255.255.255.255 ej.:

[41] Interfaz de red virtual que representa siempre al mismo dispositivo, independiente de la IP que se haya asignado a la interfaz.

Router1(config)#interface loopback 0

Router1(config-if)#

%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

Como se puede ver una vez que se llama a la interfaz esta automáticamente sube, una vez hecho esto se le pone la ip debida ejm:

Router1(config-if)#ip add 10.1.10.1 255.255.255.255

Y de esa forma queda establecida la loopback.

10.4.4 Verificación de conectividad OSPF.

Para realizar la verificación de conectividad de OSPF podemos hacer uso de varios comandos que nos podrán indicar cómo va el proceso o la adyacencia que se da en OSPF

Show ip ospf nieghbors.- Este comando nos va a mostrar los vecinos que se tiene en la topología OSPF donde se tendrán los siguientes campos:

- **ID de vecino:** La ID del router vecino
- **Pri:** la prioridad del OSPF de la interfaz
- **Estado:** el estado OSPF de la interfaz. El estado full indica que el router y su vecino poseen bases de datos de estado de enlace idénticas.
- **Tiempo muerto:** La cantidad de tiempo restante que el router tiene antes de recibir el saludo del router vecino.
- **Dirección:** La dirección IP de la interfaz del vecino a la que está directamente conectada el router
- **Interfaz:** La interfaz donde este router formó adyacencia con el vecino.

El resultado de la aplicación de este protocolo se muestra a continuación

```
Router1#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.10.1        0   FULL/  -        00:00:37    10.1.1.2        Serial0/0/0
Router1#
```

(Systems, 2012)

Otro comando que nos puede servir para determinar fallas de conectividad es el show ip OSPF

Este generalmente arroja la cantidad de LSR y LSA que se establecen en la conexión OSPF por defecto.

```
Router1#sh ip ospf
 Routing Process "ospf 1" with ID 192.168.1.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 2
        Area has no authentication
        SPF algorithm executed 9 times
        Area ranges are
```

Number of LSA 3. Checksum Sum 0x018665

Number of opaque link LSA 0. Checksum Sum 0x000000

Number of DCbitless LSA 0

Number of indication LSA 0

Number of DoNotAge LSA 0

Flood list length 0

(Systems, 2012)

Otro más que se puede utilizar es el **show ip OSPF interface.**

Router1#sh ip ospf interface

FastEthernet0/0 is up, line protocol is up

Internet address is 192.168.1.1/24, Area 0

Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 1

Transmit Delay is 1 sec, State WAITING, Priority 1

No designated router on this network

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

No Hellos (Passive interface)

Index 1/1, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 0, Adjacent neighbor count is 0

Suppress hello for 0 neighbor(s)

Serial0/0/0 is up, line protocol is up

Internet address is 10.1.1.1/30, Area 0

Process ID 1, Router ID 192.168.1.1, Network Type POINT-TO-POINT, Cost: 64

Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0

No designated router on this network

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:07

Index 2/2, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 1 , Adjacent neighbor count is 1

Adjacent with neighbor 10.10.10.1

Suppress hello for 0 neighbor(s)

Router1#

(Systems, 2012)

Es posible que dos routers no formen adyacencia OSPF si:

- Las máscaras de subred no coinciden, Si los temporizadores de saludo y muerto no coinciden.
- Si los temporizadores de saludo y muerto no coinciden
- Si los tipos de redes OSPF no coinciden
- Hay algún comando network que no ha sido declarado o esta incorrecto.

Hay que tener mucho cuidado al momento de establecer el ID del router pues cuando hay dos ID duplicadas esto causa que el enrutamiento entre estas interfaces falle.

Para verificar la adyacencia de OSPF y su funcionamiento también es muy útil el show IP route, este comando nos permite verificar las rutas recibidas por OSPF

Router1#sh 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

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks

C 10.1.1.0/30 is directly connected, Serial0/0/0

C 10.1.10.1/32 is directly connected, Loopback0

O 10.10.10.0/30 [110/128] via 10.1.1.2, 01:06:39, Serial0/0/0

C 192.168.1.0/24 is directly connected, FastEthernet0/0

O 192.168.10.0/24 [110/129] via 10.1.1.2, 01:04:55, Serial0/0/0

(Systems, 2012)

Como se puede observar en lo resaltado con amarillo se ven las rutas recibidas con la letra O estas son las rutas recibidas por OSPF.

10.4.5 Métrica de OSPF

La métrica de OSPF se da como costo, siempre se va a elegir por defecto la ruta con menor costo. El sistema operativo de cisco usa los anchos de banda acumulados en las interfaces desde el router hasta la red de destino como valor de costo. El costo de una de las interfaces se calcula:

$$Costo = (10^8 * Bw)$$

Donde el Bw es en ancho de banda de referencia.

Para ver como se calcula el costo con otros anchos de banda **(Ver figura 6).**

10.4.6 Ancho de banda de referencia

El ancho de banda de referencia es siempre de 1Mbps y más con el costo de OSPF en 1, esto se puede modificar mediante el comando **auto-cost reference-bandwidth** de OSPF.

10.4.6.1 Costos OSPF

10.4.6.1.1 OSPF acumula costos

El costo de una ruta como se mencionó anteriormente es el valor acumulado desde el router de partida hasta la red destino. **(Ver figura 7)**

10.4.7 Ancho de banda en interfaces seriales.

El valor por defecto para las interfaces seriales en los routers cisco es de 1.544 Kbps sin embargo ciertas interfaces pueden tener otros valores por defecto de 128 Kbps. Por eso es necesario siempre chequear el valor por defecto mediante el comando show interfaces.

10.4.8 Modificación del costo del enlace.

La modificación manual es posible, siempre y cuando ambos puntos de la interface se modifiquen en este valor, esto se logra mediante esto se logra mediante el comando **bandwidth** o modificando directamente el costo con **ip ospf cost**

10.5 Resumen del capitulo

Según lo visto en este capítulo podemos concluir

- OSPF es un protocolo de estado de enlaces
- Se descubre a los vecinos usando un protocolo denominado Hello
- Se establecen las adyacencias y las bases de datos de estados de enlaces son s incronizadas
- Se propagan Anuncios de Estado de Enlaces (LSA) a través de intercambios e ntre vecinos
- Se realiza una sincronización global de enlaces y en cada nodo se construye e l grafo de la red
- Se calculan caminos mínimos y las tablas de enrutamiento

Capítulo 11

11 Conclusiones y recomendaciones

11.1 Conclusiones

- Los protocolos son conjuntos de reglas que se establecen para poder llegar a un fin común.
- Existen 2 tipos de enrutamiento el Estático y el Dinámico
- El enrutamiento estático es utilizado solo en redes pequeñas pues en redes de gran magnitud se vuelve tediosa su configuración.

- El enrutamiento dinámico es un tipo de enrutamiento que facilita la obtención de rutas por medio de la propagación de una tabla de enrutamiento que contendría cualquier cambio que se realice en la red
- RIP es un protocolo con clase por lo que no se recomienda su uso en redes pequeñas no orientadas a la conexión.
- Es importante que todos los routers dentro de una red utilicen el mismo protocolo de enrutamiento dinámico, es decir mismo protocolo y versión pues si se utilizan distintos esto causaría la falla al momento de la convergencia de la red.
- EIGRP es un protocolo sin clase orientado a la conexión, es decir este podrá reconocer redes subneteadas haciendo un mejor uso de la distribución de un rango de IP definidas.
- OSPF es un protocolo que se basa en áreas de comunicación y cuya tabla de enrutamiento además incluye la wildcard de la red que es un inverso de la máscara de subred haciendo a este protocolo un protocolo de fácil convergencia y fuerte para su aplicación.

11.2 Recomendaciones

- Es muy importante fijarse un protocolo de enrutamiento debido al momento de levantar una red o de diseñarla.

- Se recomienda en su mayoría realizar las configuraciones en físico pues no es lo mismo tener las posibles fallas de un mal funcionamiento de algún cable lo cual nos entrena para poder detectar fallas de todo tipo.
- Es recomendable al momento de detectar una falla seguir las capas del modelo OSI de esta manera se detecta cualquier falla mucho más rápida y efectivamente.

Figuras

Capítulo 1

Figura 1 (malla curricular UCSG)

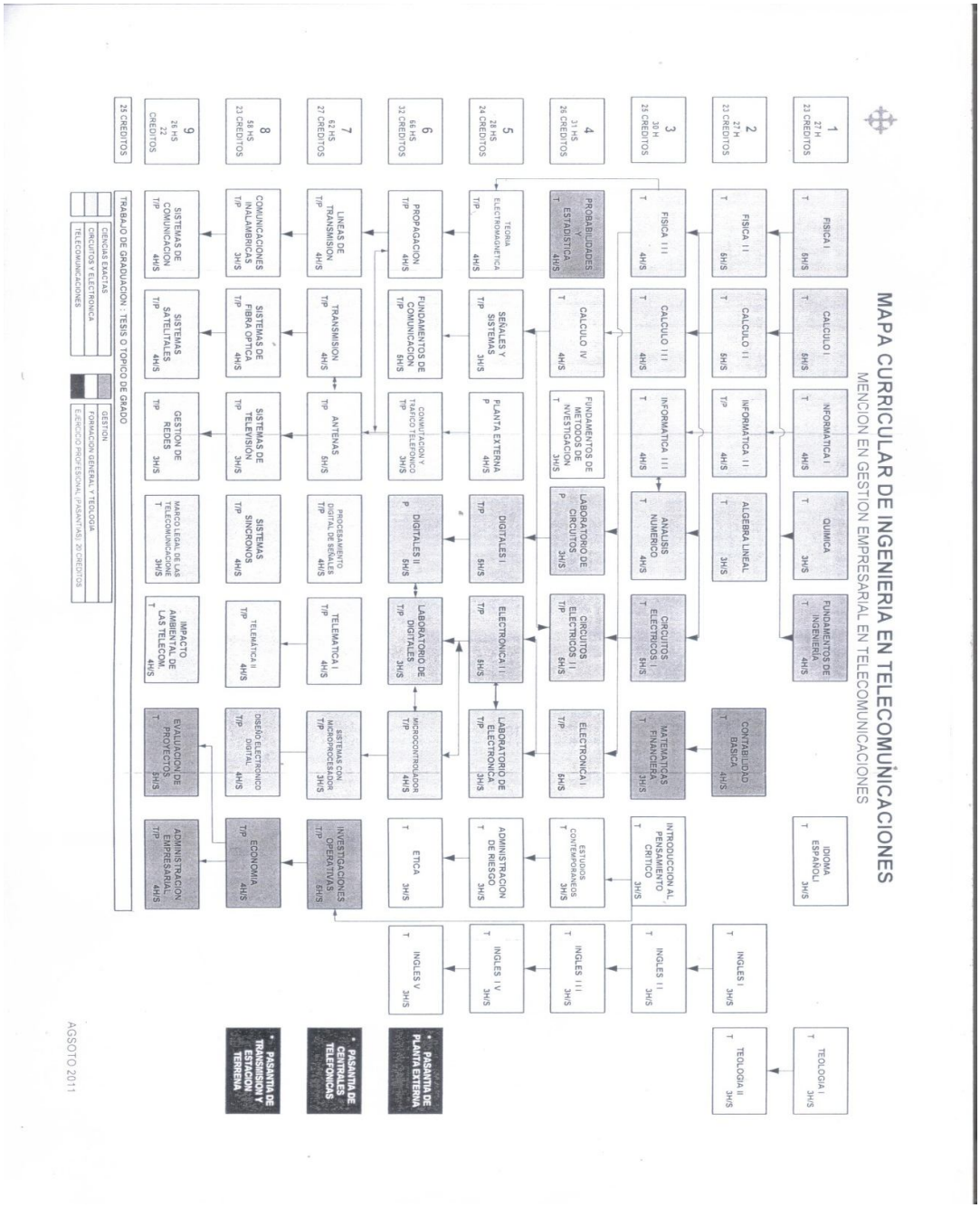
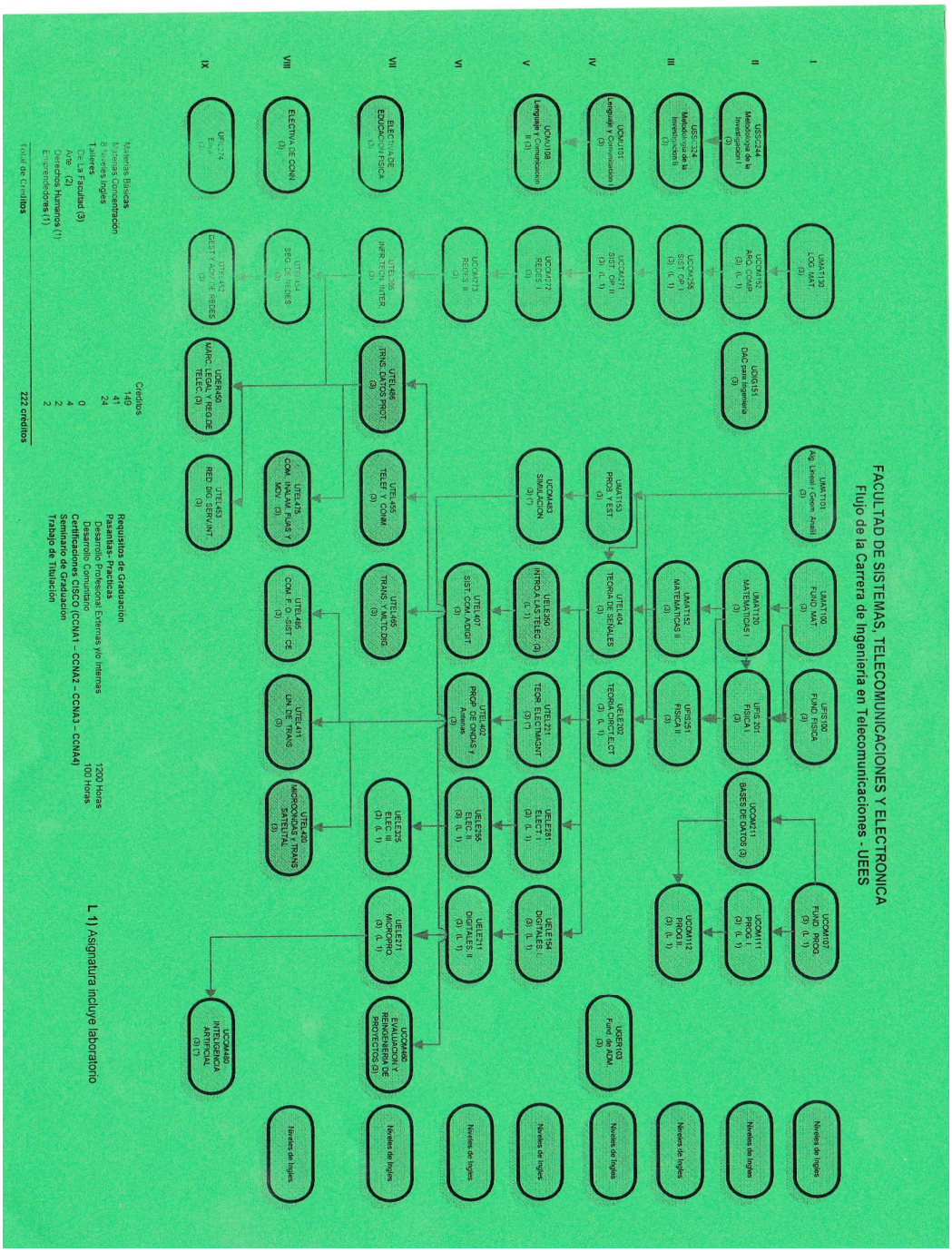


Figura 2 (Malla curricular UEES)

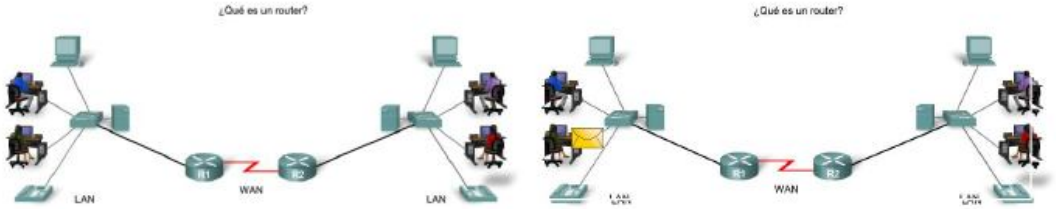
Malla curricular Ingeniería en Telecomunicaciones UEES



Capítulo 2

Figura 1 (Generalidades del router)

1841 Enrutador de servicios integrados



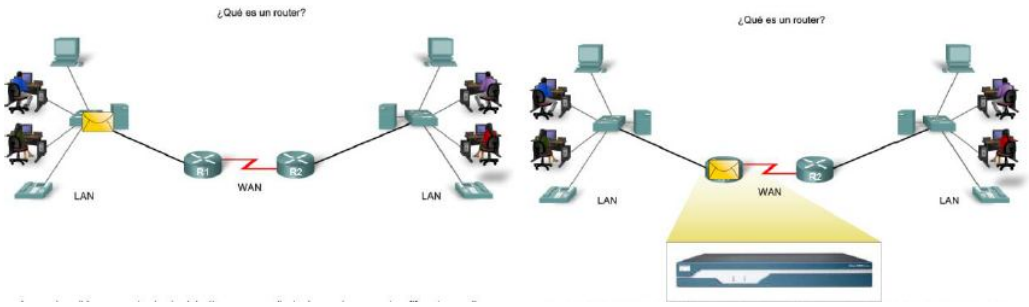


Figura 2 (Variación de VLSM)

Cisco Semester 5 — VLSM Chart

Class C Subnet Table	/24 .0 (00000000) 0 subnets/254 hosts	/25 .128 (10000000) 0 subnet 126 hosts	/26 .192 (11000000) 2 subnets 62 hosts	/27 .224 (11100000) 6 subnets 30 hosts	/28 .240 (11110000) 14 subnets14 hosts	/29 .248 (11111000) 30 subnets 6 hosts	/30 .252 (11111100) 62 subnets 2 hosts
.0	.0	.0	.0	.0	.0	.0	.0 (.1 -.2)
.4						(.1 - .6)	.4 (.5 - .6)
.8					(.1 - .14)	.8	.8 (.9 - .10)
.12				(.1 - .30)		(.9 - .14)	.12 (.13 - .14)
.16					.16	.16	.16 (.17 - .18)
.20						(.17 - .22)	.20 (.21 - .22)
.24					(.17 - .30)	.24	.24 (.25 - .26)
.28			(.1 - .62)			(.25 - .30)	.28 (.29 - .30)
.32				.32	.32	.32	.32 (.33 - .34)
.36						(.33 - .38)	.36 (.37 - .38)
.40					(.33 - .46)	.40	.40 (.41 - .42)
.44				(.33 - .62)		(.41 - .46)	.44 (.45 - .46)
.48					.48	.48	.48 (.49 - .50)
.52						(.49 - .54)	.52 (.53 - .54)
.56					(.49 - .62)	.56	.56 (.57 - .58)
.60		(.1 - .126)				(.57 - .62)	.60 (.61 - .62)
.64			.64	.64	.64	.64	.64 (.65 - .66)
.68						(.65 - .70)	.68 (.69 - .70)
.72					(.65 - .78)	.72	.72 (.73 - .74)
.76				(.65 - .94)		(.73 - .78)	.76 (.77 - .78)
.80					.80	.80	.80 (.81 - .82)
.84						(.81 - .86)	.84 (.85 - .86)
.88					(.81 - .94)	.88	.88 (.89 - .90)
.92			(.65 - .126)			(.89 - .94)	.92 (.93 - .94)
.96				.96	.96	.96	.96 (.97 - .98)
.100						(.97 - .102)	.100 (.101 - .102)
.104					(.97 - .108)	.104	.104 (.105 - .106)
.108				(.97 - .126)		(.105 - .108)	.108 (.107 - .108)
.112					.112	.112	.112 (.113 - .114)
.116						(.113 - .118)	.116 (.117 - .118)
.120					(.113 - .126)	.120	.120 (.121 - .122)
.124						(.121 - .126)	.124 (.125 - .126)
.128	(.1 - .254)	.128	.128	.128	.128	.128	.128 (.129 - .130)
.132						(.129 - .130)	.132 (.133 - .134)
.136					(.129 - .142)	.136	.136 (.137 - .138)
.140				(.129 - .158)		(.137 - .142)	.140 (.141 - .142)
.144					.144	.144	.144 (.145 - .146)
.148						(.145 - .150)	.148 (.149 - .150)
.152					(.145 - .158)	.152	.152 (.153 - .154)
.156			(.129 - .191)			(.153 - .158)	.156 (.157 - .158)
.160				.160	.160	.160	.160 (.161 - .162)
.164						(.161 - .166)	.164 (.165 - .166)
.168					(.161 - .174)	.168	.168 (.169 - .170)
.172				(.161 - .190)		(.169 - .174)	.172 (.173 - .174)
.176					.176	.176	.176 (.177 - .178)
.180						(.177 - .182)	.180 (.181 - .182)
.184					(.177 - .190)	.184	.184 (.185 - .186)
.188						(.185 - .190)	.188 (.189 - .190)
.192		(.129 - .254)	.192	.192	.192	.192	.192 (.193 - .194)
.196						(.193 - .198)	.196 (.197 - .198)
.200					(.193 - .206)	.200	.200 (.201 - .202)
.204				(.193 - .222)		(.201 - .206)	.204 (.205 - .206)
.208					.208	.208	.208 (.209 - .210)
.212						(.209 - .214)	.212 (.213 - .214)
.216					(.209 - .222)	.216	.216 (.217 - .218)
.220			(.191 - .254)			(.217 - .222)	.220 (.221 - .222)
.224				.224	.224	.224	.224 (.225 - .226)
.228						(.225 - .230)	.228 (.229 - .230)
.232					(.225 - .238)	.232	.232 (.233 - .234)
.236				(.225 - .254)		(.233 - .238)	.236 (.237 - .238)
.240					.240	.240	.240 (.241 - .242)
.244						(.241 - .246)	.244 (.244 - .246)
.248					(.241 - 254)	.248	.248 (.249 - .250)
.252						(.249 - .254)	.252 (.253 - .254)

Capítulo 3

Figura 1 (Cable serial normativa RS232)

CABLE CONECTOR DB25

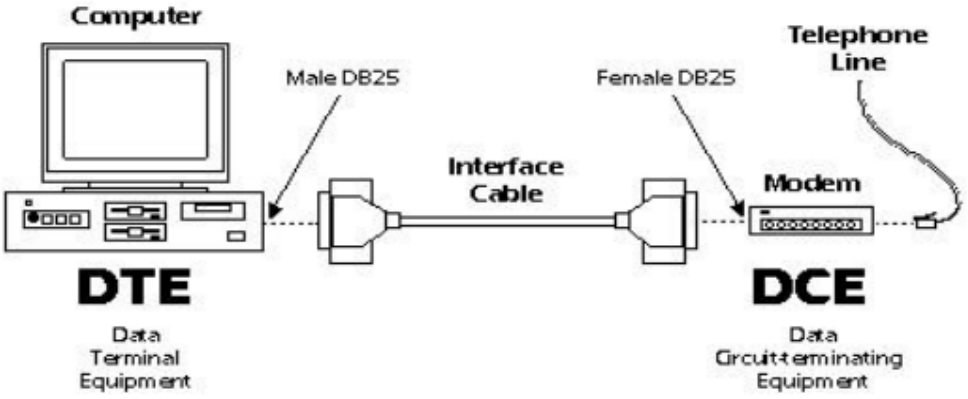


Figura 2 (Función de Pines de conector serial DB25)

Función de los pines en el conector DB-25			
No. Pin	**Nombre**	**Función**	**Dirección**
1		Protección a tierra	-
2	TX	Transmisión de datos	DTE-DCE
3	RX	Recepción de datos	DCE-DTE
4	RTS	Request to send -Petición para enviar	DTE-DCE
5	CTS	Clear to send -Listo para enviar	DCE-DTE
6	DSR	Data Set Ready -DCE listo	DCE-DTE
7	GND	Tierra	-
8	DCD	Data Carrier Detect -Detección de portadora	DCE-DTE
9		Reservado para test	
10		Reservado para test	
11		Sin asignar	

Función de los pines en el conector DB-25			
No. Pin	**Nombre**	**Función**	**Dirección**
12	DCD 2	Data Carrier Detect- Detección de portadora del canal secundario	DCE-DTE
13	CTS 2	Clear to send -Listo para enviar del canal secundario	DCE-DTE
14	TX 2	Transmisión de datos del canal secundario	DTE-DCE
15	TC	Temporización (reloj) de transmisión (modo síncrono)	DCE-DTE
16	RX 2	Recepción de datos del canal secundario	DCE-DTE
17	RC	Temporización (reloj)de recepción (modo síncrono)	DCE-DTE
18		Bucle local	DTE-DCE
19	RTS 2	Request to Send -Petición para enviar del canal secundario	DTE-DCE
20	DTR	Data Terminal Ready -DTE listo	DTE-DCE
21	SQ	Signal Quality -Bucle local y detector de calidad de la señal	DTE-DCE
22	RI	Ring Indicator -Indicador llamada entrante	DCE-DTE

Función de los pines en el conector DB-25			
No. Pin	**Nombre**	**Función**	**Dirección**
23		Selector de Velocidad del DTE	DTE-DCE
24	XTC	Temporización (reloj) de transmisión (modo síncrono)	DTE-DCE
25		Reservado para test	

Figura 3 (Norma EIA 449)

NORMA EIA 449

Figura 4 (Normativa V.35)

V.35	
BW	Distancia (m)
2 Mb/s	45.72
1 Mb/s	91.4
512 Kb/s	182.9
256 Kb/s	365.8
128 Kb/s	731.5
56 Kb/s	914.4
1.2 Kb/s	914.4

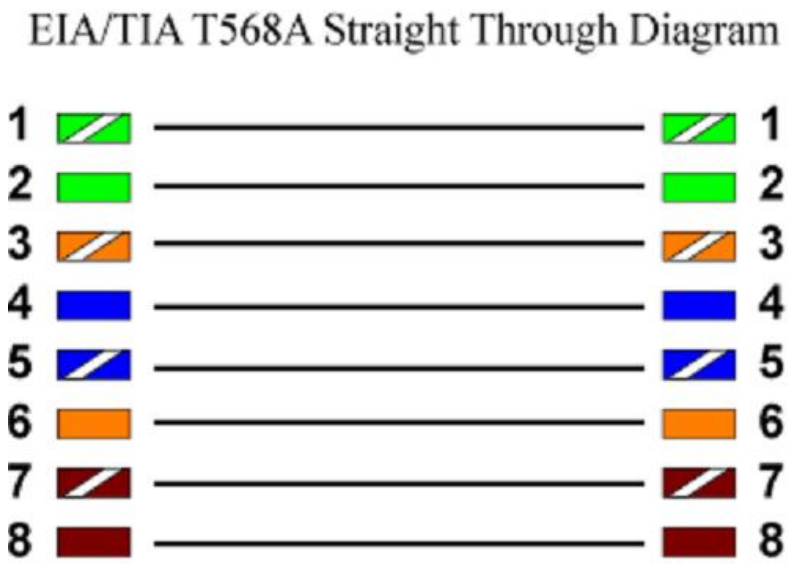
Tabla de distancia vs ancho de banda para v.35

Figura 5 (conector DB-15- MRAC-34)

Conector DB-15

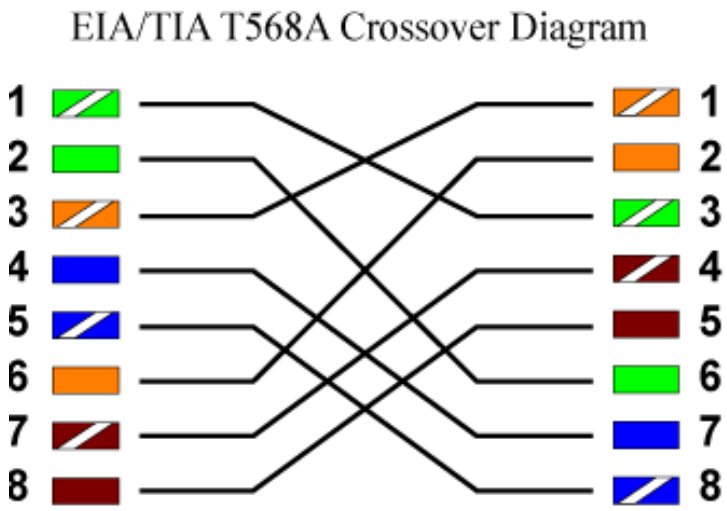
Conector MRAC-34

Figura 6 (Normativa de conexión para cable directo



Configuración T568A

Figura 7 (Normativa de conexión de cable cruzado)



Conexión Cruzada T568A y T568B

Figura 8 (Tabla de enrutamiento)

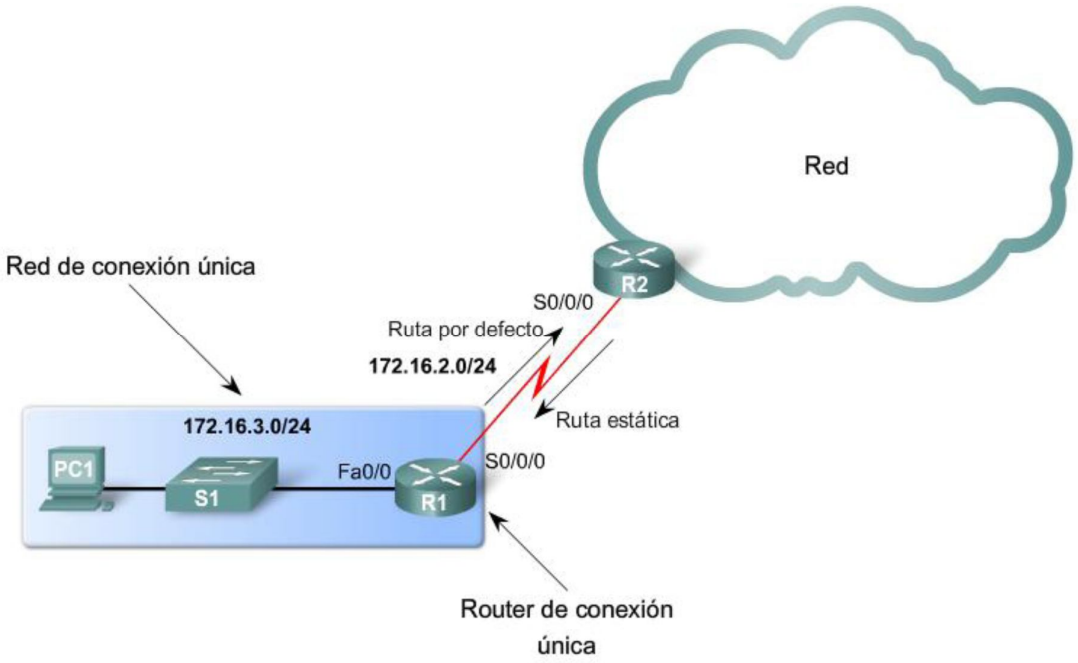
```
Router>sho ip rou
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       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

C    192.168.0.0/24 is directly connected, FastEthernet0/1
C    192.168.1.0/24 is directly connected, Serial0/0/0
Router>
```

TABLA DE ENRUTAMIENTO CISCO

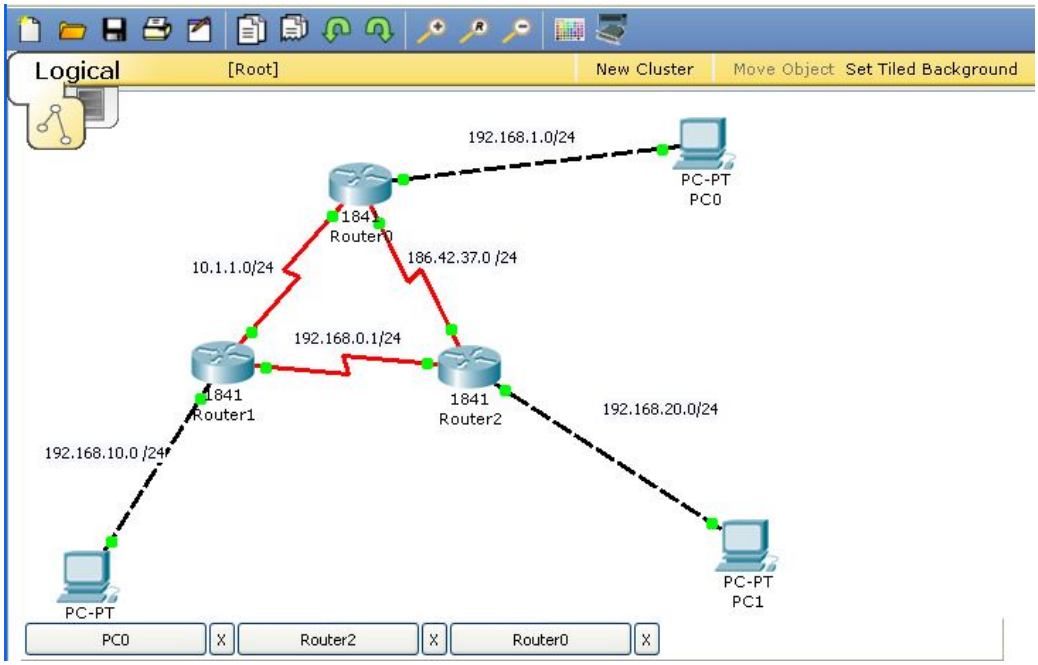
Figura 9 (Ruta al ISP)



Conexión única.

Capítulo 4

Figura 1 (Topología ejemplo de Distancia Administrativa)



Capítulo 5

Figura 1 (Características clave de RIP)

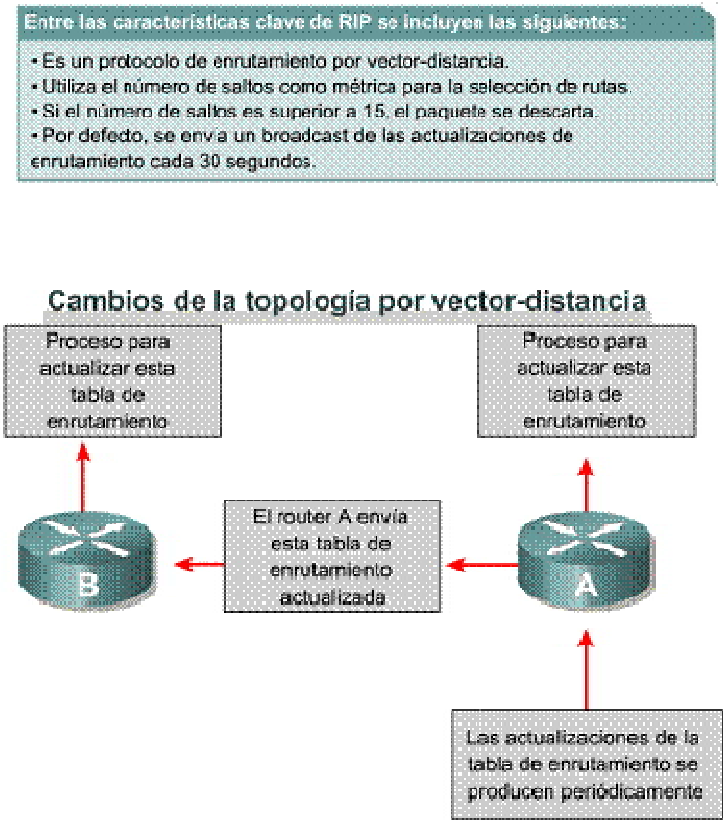
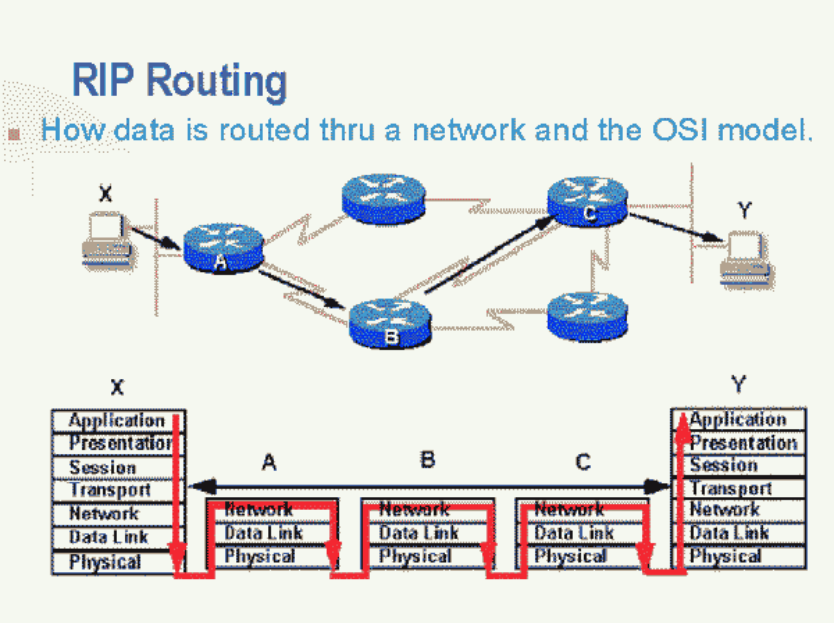
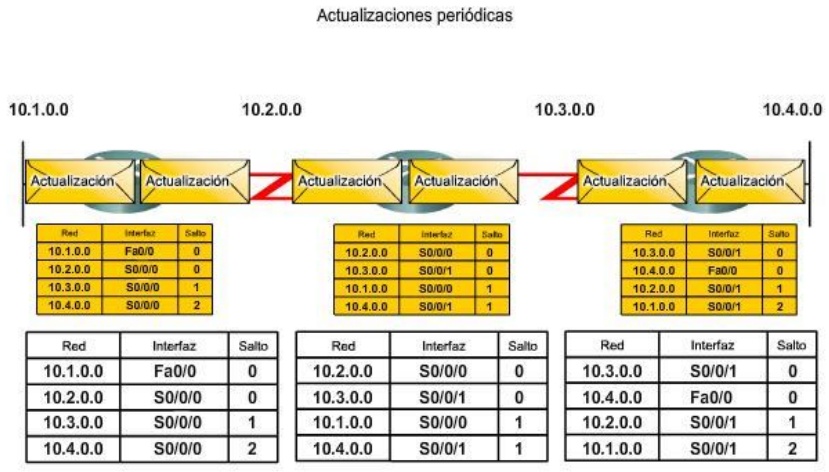


Figura 2 (Cómo la data pasa a través del modelo OSI)



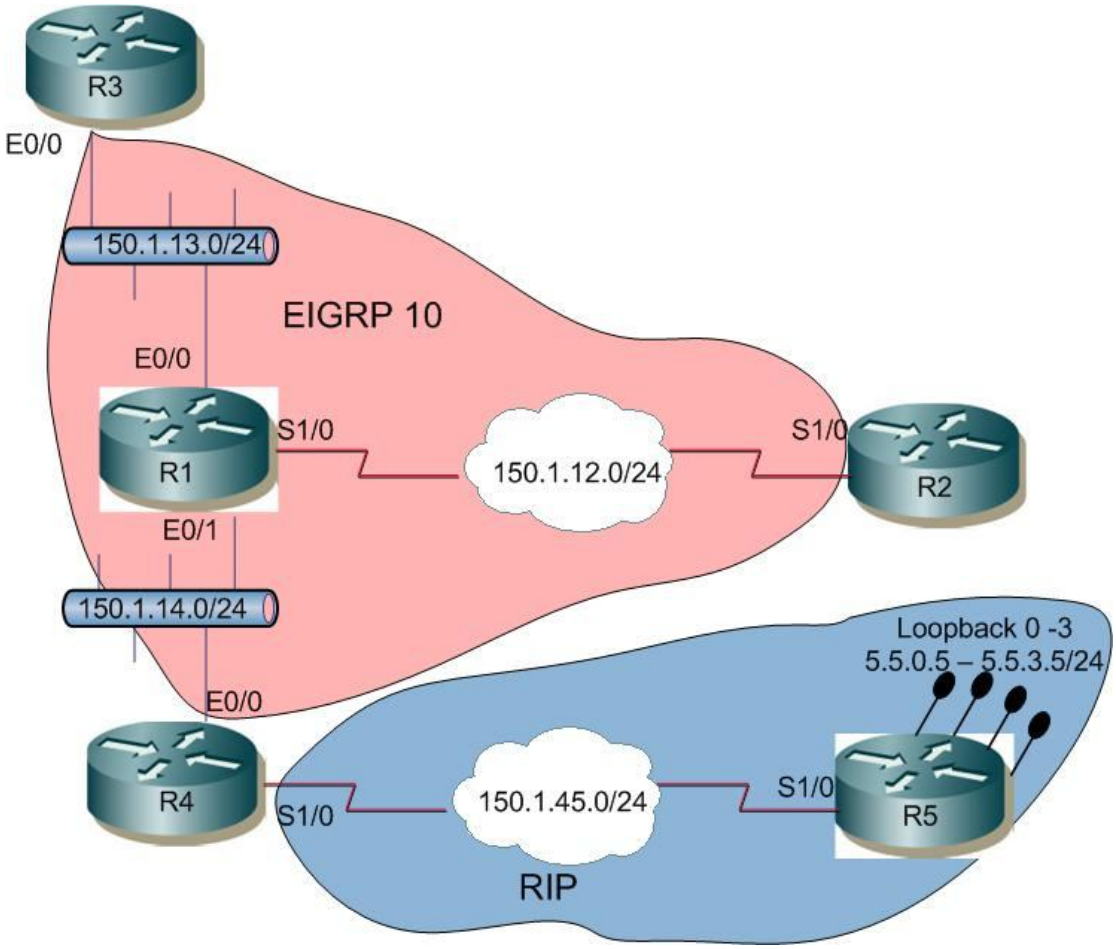
Como se enruta los paquetes en la red y el modelo OSI

Figura 3 (Actualizaciones de RIP)



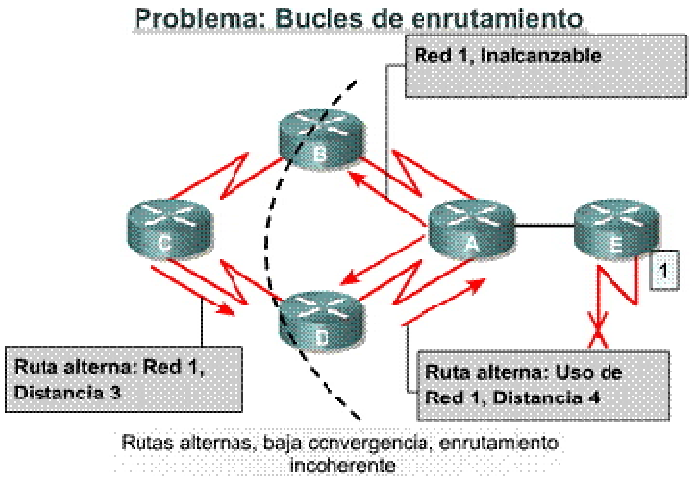
ACTUALIZACIONES RIP

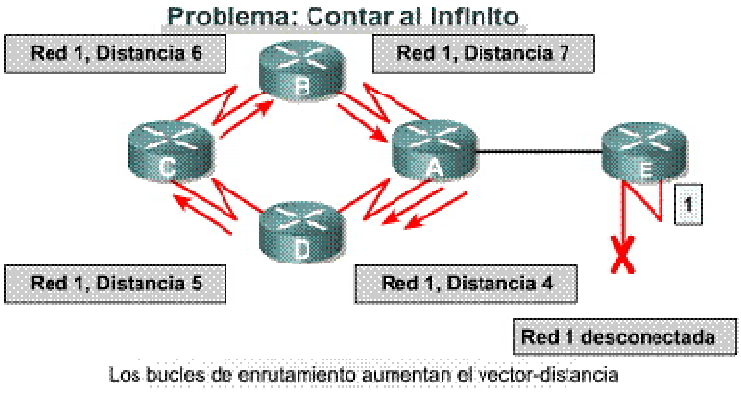
Figura 4 (Topología de una red con protocolos EIGRP y RIP)



Topología de una red con protocolos EIGRP y RIP

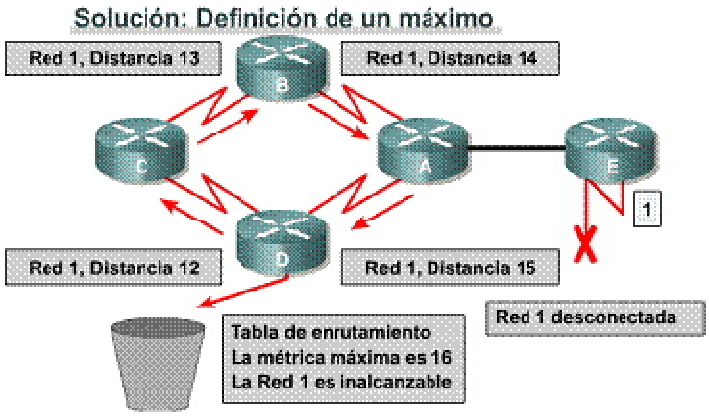
Figura 5 (problemas de bucles de enrutamiento (routing loops))





Rooting loops

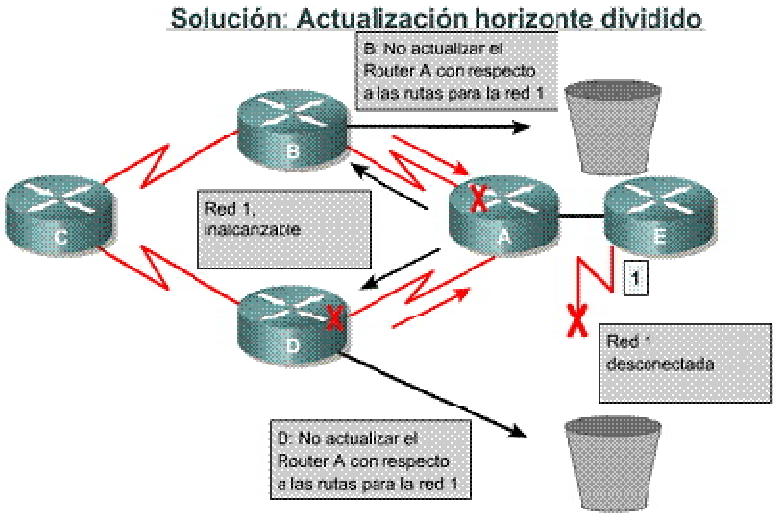
Figura 6 (Métrica máxima)



Especificar una métrica de vector-distancia máximo como infinito

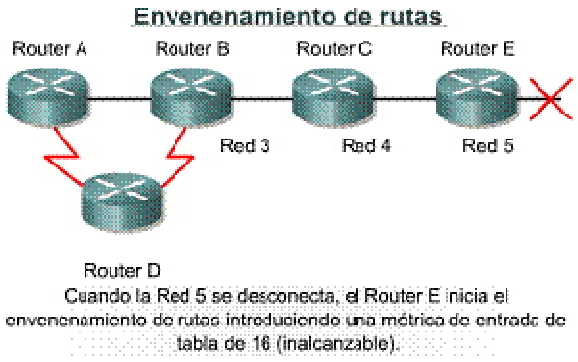
MÉTRICA MÁXIMA

Figura 7 (Horizonte Dividido)



HORIZONTE DIVIDIDO

Figura 8 (Envenenamiento de rutas)



ENVENENAMIENTO DE RUTAS

Figura 9 (Temporizadores de espera)

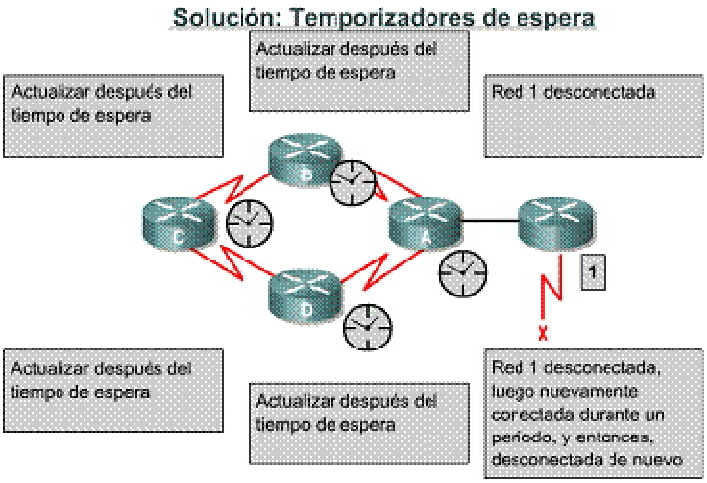
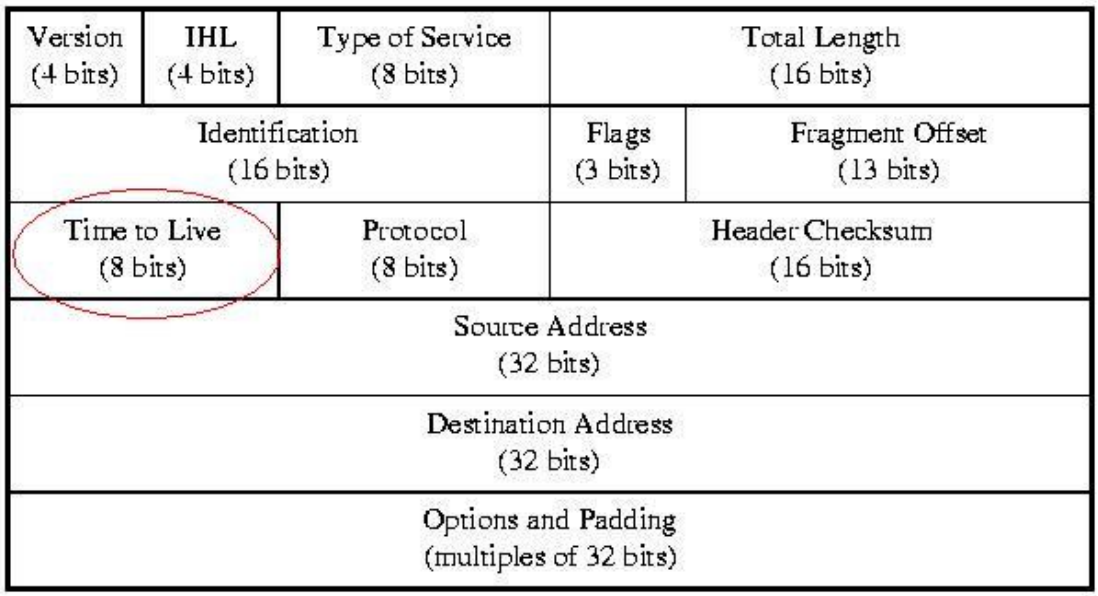


Figura 10 (Datagrama IP, TTL)

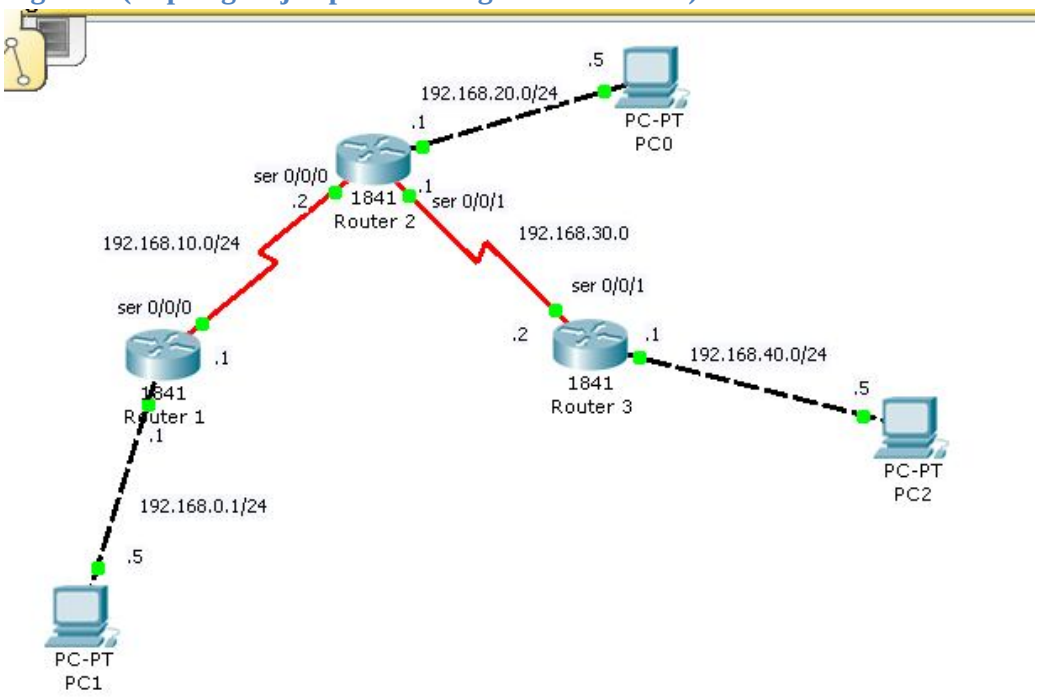


DATAGRAMA IP, CAMPO TTL

Capítulo 6

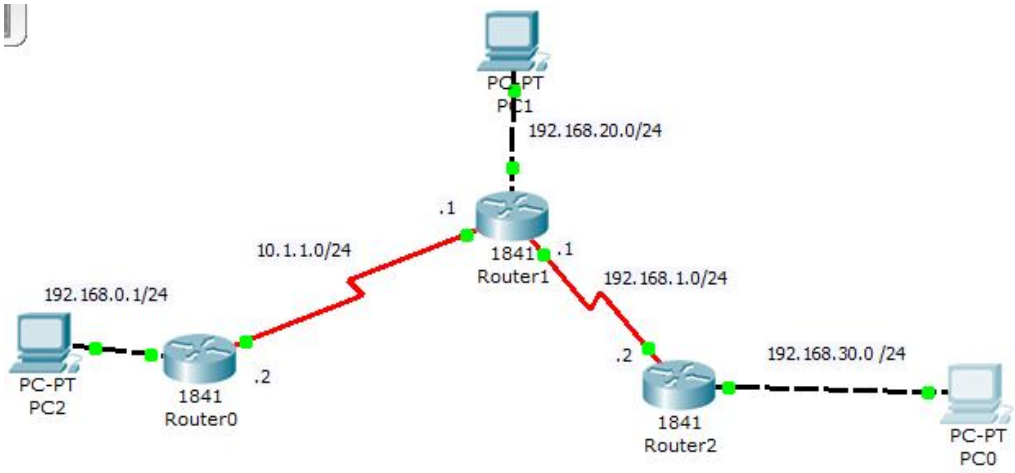
Figura 1(Formato del mensaje RIP v1)

Figura 2 (Topología ejemplo de configuración RIP v1)



Capítulo 7

Figura 1 (Topología ejemplo de configuración RIP v2)



Capítulo 8

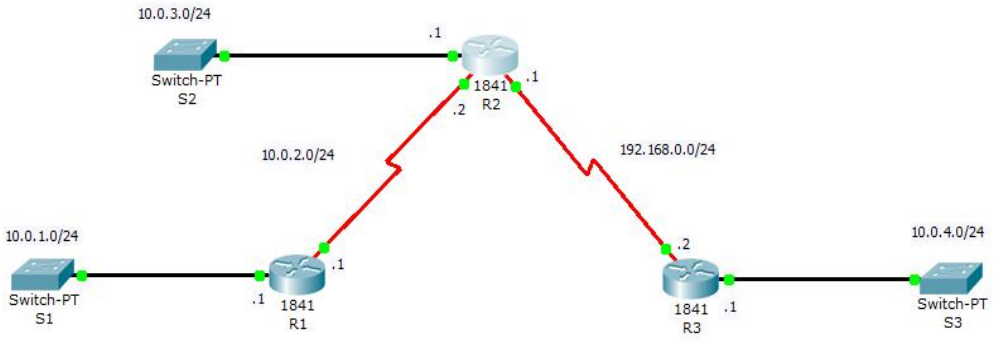
Figura 1 (información de la tabla de enrutamiento)

RRAS-1 - IP Routing Table

Destino	Máscara de red	Puerta de e...	Interfaz	Métrica	Protocolo
192.168.10.0	255.255.255.0	192.168.01	192.168	1	Static (non demand-dial)
192.168.0.0	255.255.255.0	192.168.01	192.168	2	OSPF
10.199.17.0	255.255.255.0	10.199.1780	Corpnet	2	OSPF
0.0.0.0	0.0.0.0	10.199.171	Corpnet	2[	Network management
255.255.255.255	255.255.255.255	192.100.01	192.100	1	Local
255.255.255.255	255.255.255.255	172.16.0.1	172.16	1	Local

Información de la Tabla de enrutamiento.

Figura 2 (Topología ejemplo rutas primarias y secundarias)




```
Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 2 subnets
C       10.0.2.0 is directly connected, Serial0/0/0
C       10.0.3.0 is directly connected, FastEthernet0/0
C    192.168.0.0/24 is directly connected, Serial0/0/1
R2#
```

Diseño de red para explicación de tabla de enrutamiento.

Figura 3 (Ejemplo de red sin VLSM)

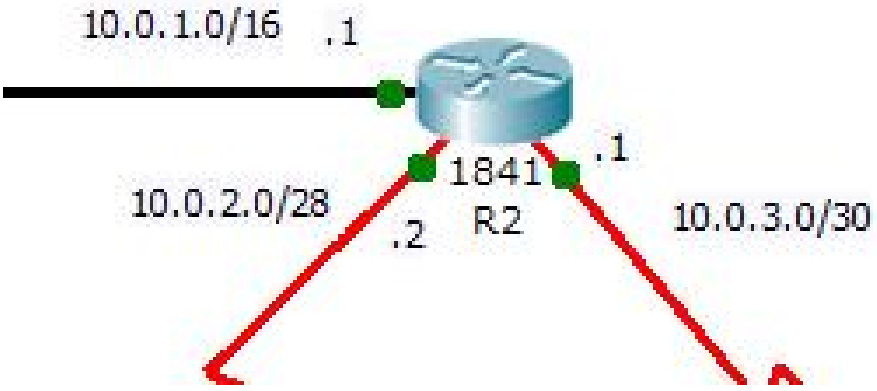


Figura 4 (Topología ejemplo tabla de enrutamiento de RIP)

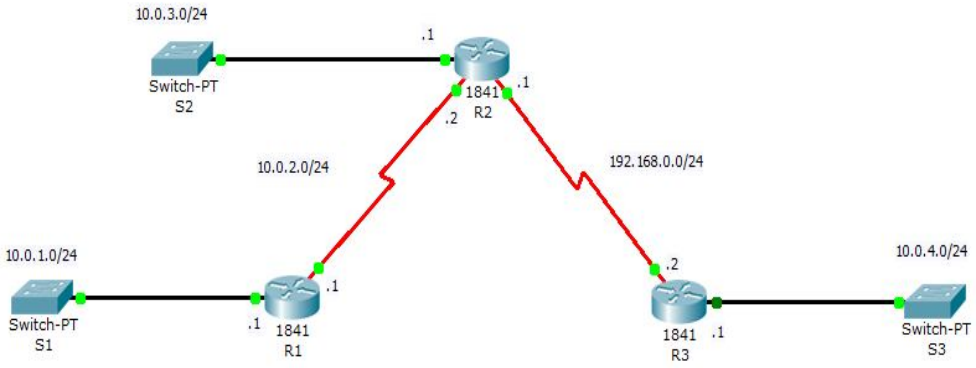
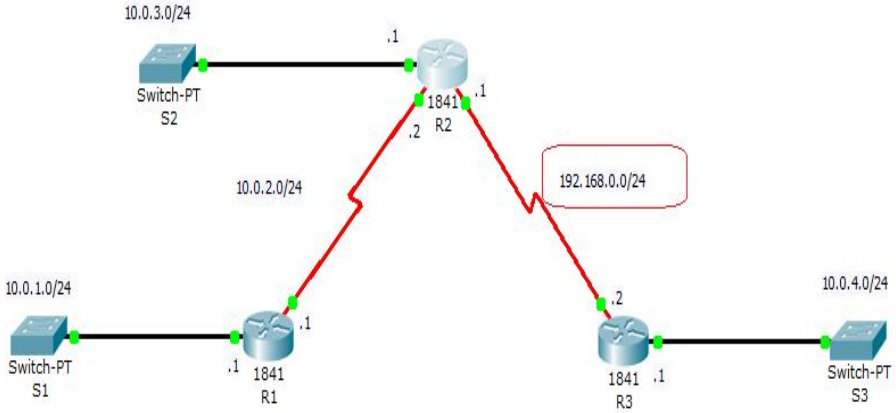


Figura 5 (Topología ejemplo RIP enrutamiento con clase)



Capítulo 9

Figura 1 (Mensaje EIGRP)

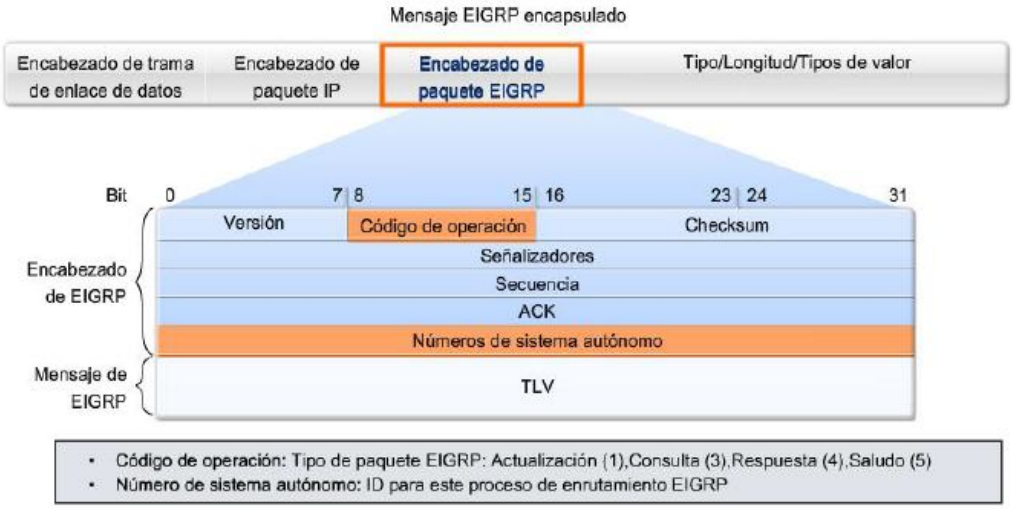
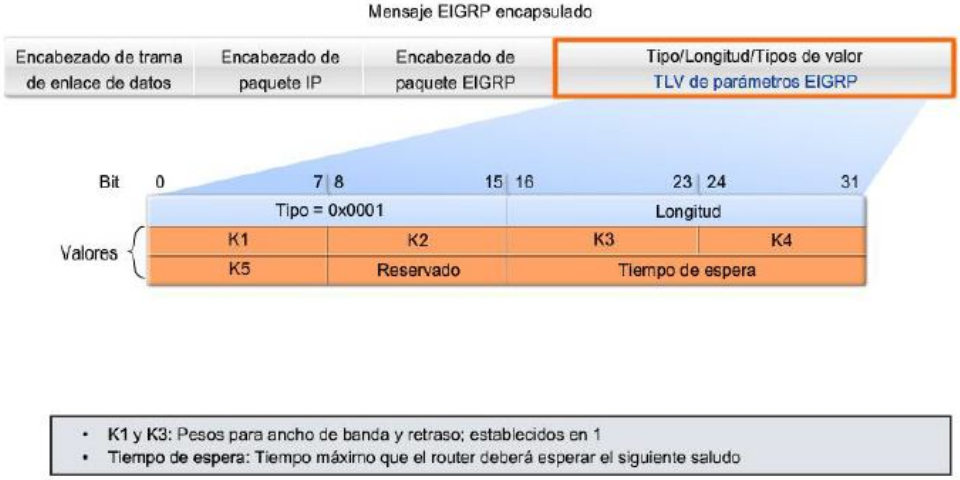


Figura 2 (mensaje EIGRP constantes)



Capítulo 10

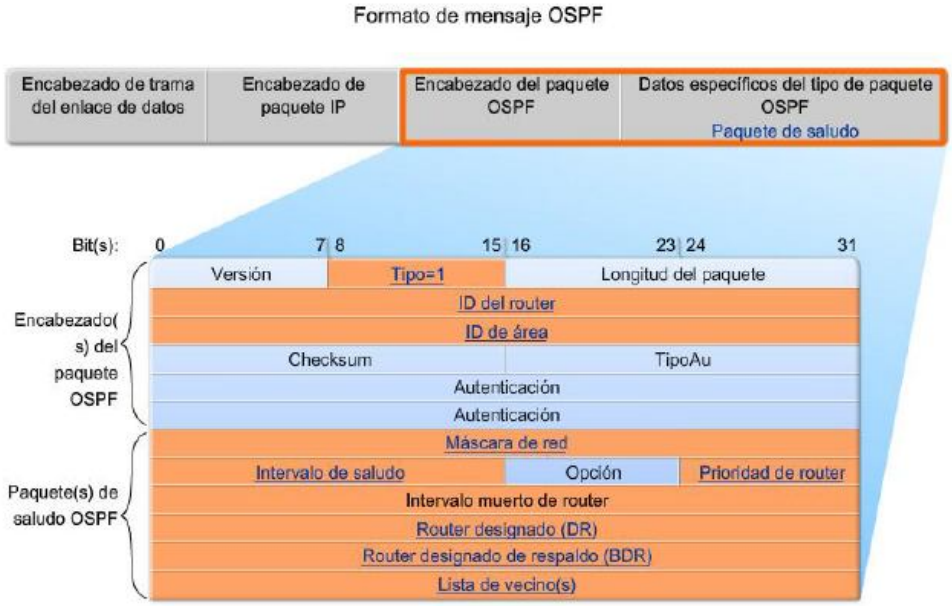
Figura 1 (Mensaje OSPF)

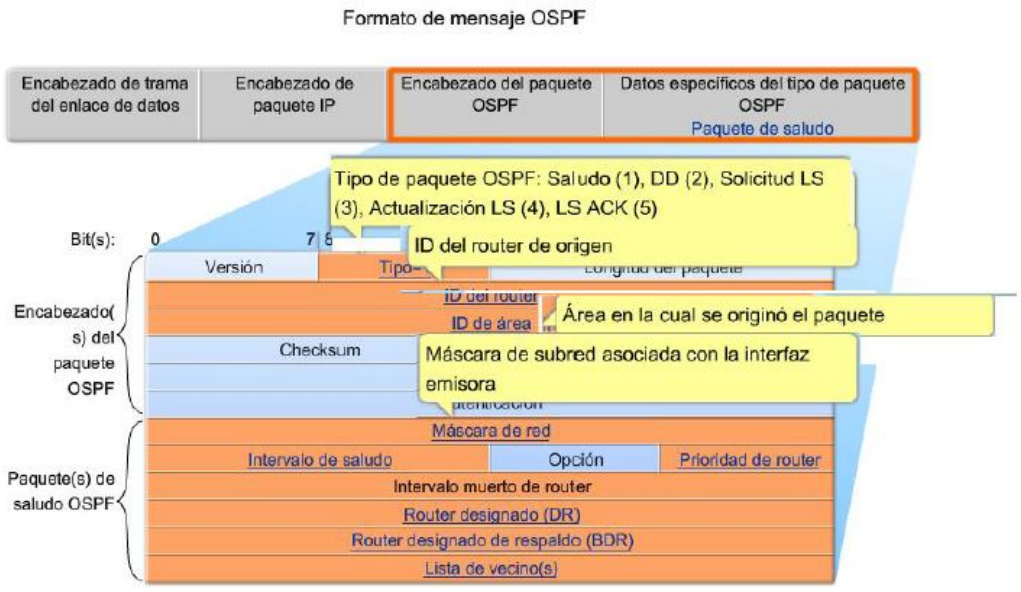
Figura 2 (Tipos de paquete OSPF)

Tipos de paquete OSPF

Tipo	Nombre del paquete	Descripción
1	Saludo	Descubre los vecinos y construye adyacencias entre ellos
2	Descripción de la base de datos (DBD)	Controla la sincronización de la base de datos entre routers
3	Solicitud de estado de enlace (LSR)	Solicita registros específicos de estado de enlace de router a router
4	Actualización de estado de enlace (LSU)	Envía los registros de estado de enlace específicamente solicitados
5	Acuse de recibo de estado de enlace (LSAck)	Reconoce los demás tipos de paquetes

Figura 3 (Formato de mensaje OSPF)





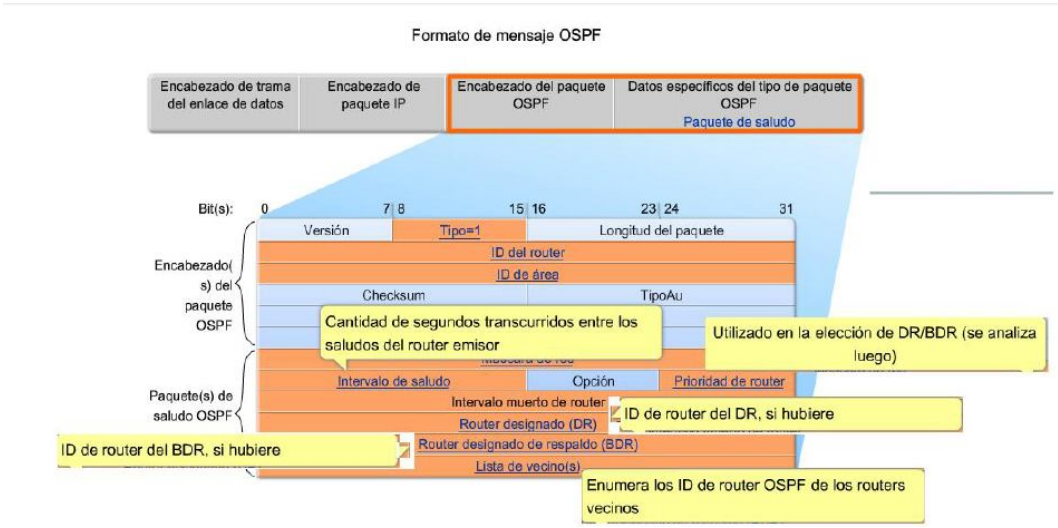


Figura 4 (LSU y LSA)

Las LSU contienen notificaciones de estado de enlace (LSA)

Tipo	Nombre del paquete	Descripción
1	Saludo	Descubre los vecinos y construye adyacencias entre ellos
2	DBD	Controla la sincronización de la base de datos entre routers
3	LSR	Solicita registros específicos de estado de enlace de router a router
4	LSU	Envía los registros de estado de enlace específicamente solicitados
5	LSAck	Reconoce los demás tipos de paquetes

- Las siglas LSA y LSU con frecuencia se utilizan indistintamente.
- Una LSU contiene una o más LSA.
- Las LSA contienen información de ruta para las redes de destino.
- La información específica de LSA se analiza en CCNP.

Tipo de LSA	Descripción
1	LSA de router
2	LSA de red
3 ó 4	LSA de resumen
5	LSA externos del sistema autónomo
6	LSA de OSPF multicast
7	Definido para áreas no tan llanas
8	Atributos externos de LSA para Border Gateway Protocol (BGP)
9, 10, 11	LSA opacas

Figura 5 (Algoritmo SPF)

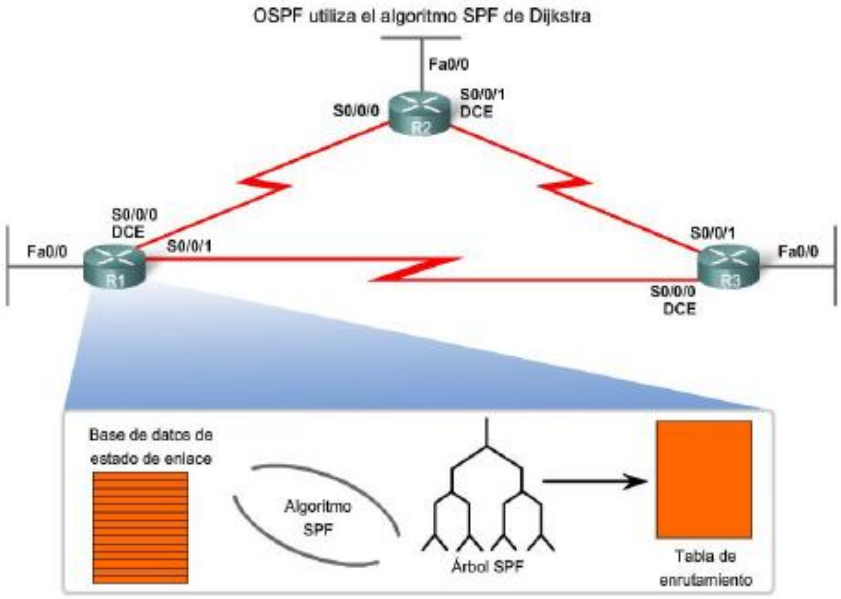
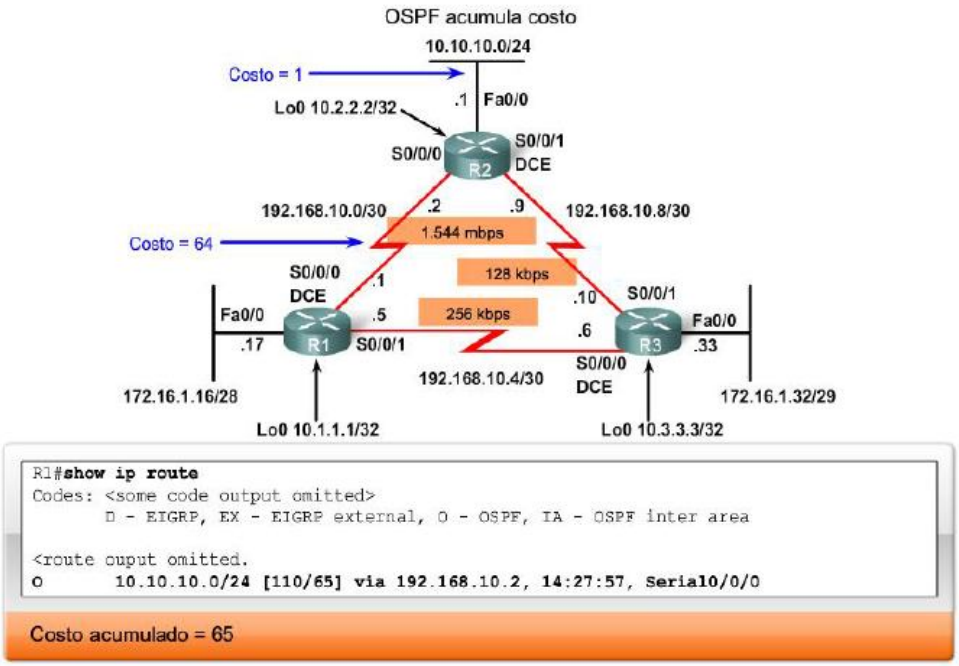


Figura 6 (Costos OSPF)

Valores de costo OSPF de Cisco

Tipo de interfaz	10^8/bps = Costo
Fast Ethernet y más rápida	10^8/100 000 000 bps = 1
Ethernet	10^8/10 000 000 bps = 10
E1	10^8/2 048 000 bps = 48
T1	10^8/1 544 000 bps = 64
128 kbps	10^8/128 000 bps = 781
64 kbps	10^8/64 000 bps = 1562
56 kbps	10^8/56 000 bps = 1785

Figura 7 (Demostración OSPF acumula costo)



Bibliografía

Cisco Systems. (15 de feb de 2009). *cisco.netacad.net.* Recuperado el 2 de marzo de 2013, de netacad.com: https://1410452.netacad.com/courses/57843

Gerometta, O. (20 de Marzo de 2010). *librosnetworking.blogspot.com*. Recuperado el 10 de febrero de 2013, de librosnetworking.blogspot.com: http://librosnetworking.blogspot.com/2010/03/distancia-administrativa.html

Gómez, G. E. (s.f.). *http://materias.fi.uba.ar/.* Recuperado el 10 de Enero de 2013, de http://materias.fi.uba.ar/: http://materias.fi.uba.ar/6679/apuntes/RS232_V35.pdf

rodri.wordpress.com. (16 de Mayo de 2007). *La bitacora de Rodri*. Recuperado el 10 de Enero de 2013, de http://rodri.wordpress.com/: http://rodri.wordpress.com/2007/05/16/cables-de-conexion-directa-y-cruzada/

Sycamore Networks, Inc. (s.f.). *http://www.networksorcery.com/*. Recuperado el 10 de Marzo de 2013, de http://www.networksorcery.com/: http://www.networksorcery.com/enp/authors/MoyJohn.htm

Teleproceso. (2010). *http://www.uazuay.edu.ec/.* Recuperado el 10 de Enero de 2013, de http://www.uazuay.edu.ec/: http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/rs449.htm

Vargas, H. A. (Octubre de 2010). *http://www.buenastareas.com/*. Recuperado el 17 de Enero de 2013, de http://www.buenastareas.com/: http://www.buenastareas.com/ensayos/Norma-Eia/995534.html

YAMID. (3 de Noviembre de 2010). *blogspot.com*. Recuperado el 15 de Enero de 2013, de blogspot.com: http://pradojah007.blogspot.com/