ENRUTAMIENTO Y CONFIGURACIÓN DE REDES

Ricardo López Bulla

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Enrutamiento y Configuración de Redes
Ricardo López Bulla
Bogotá D.C.

Fundación Universitaria del Área Andina. 2018

Catalogación en la fuente Fundación Universitaria del Área Andina (Bogotá).

Enrutamiento y Configuración de Redes

ISBN (impreso): **978-958-5462-80-9**

Fundación Universitaria del Área Andina
Calle 70 No. 12-55, Bogotá, Colombia
Tel: +57 (1) 7424218 Ext. 1231
Correo electrónico: publicaciones@areandina.edu.co

Director editorial: Eduardo Mora Bejarano
Coordinador editorial: Camilo Andrés Cuéllar Mejía
Corrección de estilo y diagramación: Dirección Nacional de Operaciones Virtuales
Conversión de módulos virtuales: Katherine Medina

BANDERA INSTITUCIONAL

Pablo Oliveros Marmolejo †
Gustavo Eastman Vélez
Miembros Fundadores

Diego Molano Vega
Presidente del Consejo Superior y Asamblea General

José Leonardo Valencia Molano
Rector Nacional
Representante Legal

Martha Patricia Castellanos Saavedra
Vicerrectora Nacional Académica

Jorge Andrés Rubio Peña
Vicerrector Nacional de Crecimiento y Desarrollo

Tatiana Guzmán Granados
Vicerrectora Nacional de Experiencia Areandina

Edgar Orlando Cote Rojas
Rector – Seccional Pereira

Gelca Patricia Gutiérrez Barranco
Rectora – Sede Valledupar

María Angélica Pacheco Chica
Secretaria General

Eduardo Mora Bejarano
Director Nacional de Investigación

Camilo Andrés Cuéllar Mejía
Subdirector Nacional de Publicaciones

ENRUTAMIENTO Y CONFIGURACIÓN DE REDES

Ricardo López Bulla

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

ÍNDICE

EJE 1

Introducción 7
Desarrollo Temático 8
Bibliografía 26

EJE 2

Introducción 28
Desarrollo Temático 29
Bibliografía 51

EJE 3

Introducción 53
Desarrollo Temático 54
Bibliografía 68

EJE 4

Introducción 70
Desarrollo Temático 71
Bibliografía 91

ENRUTAMIENTO Y CONFIGURACIÓN DE REDES

Ricardo López Bulla

EJE 1

Conceptualicemos

AREANDINA
Fundación Universitaria del Área Andina
MIEMBRO DE LA RED ILUMNO

Fuente: Shutterstock/258980774

INTRODUCCIÓN

Al introducirnos en el mágico mundo de las redes informáticas nos damos cuenta de que los avances que se han originado en torno a estas desde su **advenimiento** han sido significativos, a tal punto que hoy en día cualquier organización posee una red dentro de su esquema para garantizar correctas y efectivas comunicaciones, así como seguridad.

Esta situación da razones para estar a la vanguardia en los elementos que componen las redes, partiendo en esta oportunidad de los **dispositivos de interconexión**, su implementación e importancia, y teniendo presente la relevancia de estos en el funcionamiento de las redes. Estos dispositivos cumplen un papel fundamental en las redes convergentes, término asociado a la participación de servicios (voz-dato-video) en un mismo medio, lo cual permite a los diferentes **ISP** brindar esta tecnología a sus miles de usuarios en todo el mundo y da a las empresas la posibilidad de desarrollar sus operaciones en cualquier momento y lugar con efectividad y productividad.

En este eje temático se abordarán los aspectos básicos y de configuración de los dispositivos de interconexión a redes conmutadas y convergentes.

Advenimiento

Se entiende como la llegada de algo... un suceso o un acontecimiento.

Dispositivos de interconexión

Elementos que permiten la comunicación en las redes informáticas.

ISP

Siglas de internet service provider (proveedor de servicios de internet).

¿Qué es un dispositivo de interconexión?

Se conoce como dispositivo de interconexión el elemento que permite comunicar o interconectar dos o más dispositivos y facilita la conexión de segmentos y los terminales, característica vital para la comunicación en una red. Estos elementos son la parte del *hardware* dentro de la red.

Estos terminales o dispositivos finales, que suelen llamarse *hosts*, permiten el acceso a la red informática entre dos elementos claves: el usuario y la red. Entre los dispositivos finales encontramos PC (escritorio, portátiles), tabletas, *smartphones*, impresoras, teléfonos con tecnología IP (VOIP), cámaras para circuito cerrado, etc.

Introduciéndonos en las redes informáticas encontramos que cada *host* tiene una característica que lo hace único. Vamos a analizar esto con una analogía: cada ser humano sobre la tierra tiene un número de identificación, lo mismo pasa con los *hosts*, pero relacionándolos con una única dirección IP, la cual se aloja en el origen y el destino del mensaje a través de todo el proceso de encapsulación y desencapsulación en la red.

Segmentos
Grupo de equipos interconectados dentro de una red informática.

VOIP
Siglas de voice over internet protocol (voz a través de internet). Esta tecnología permite comunicaciones mediante el protocolo IP.

Encapsulación
Proceso que nos permite mantener un orden en el proceso de la comunicación partiendo del origen de los datos hasta su destino, garantizando la entrega del mensaje.

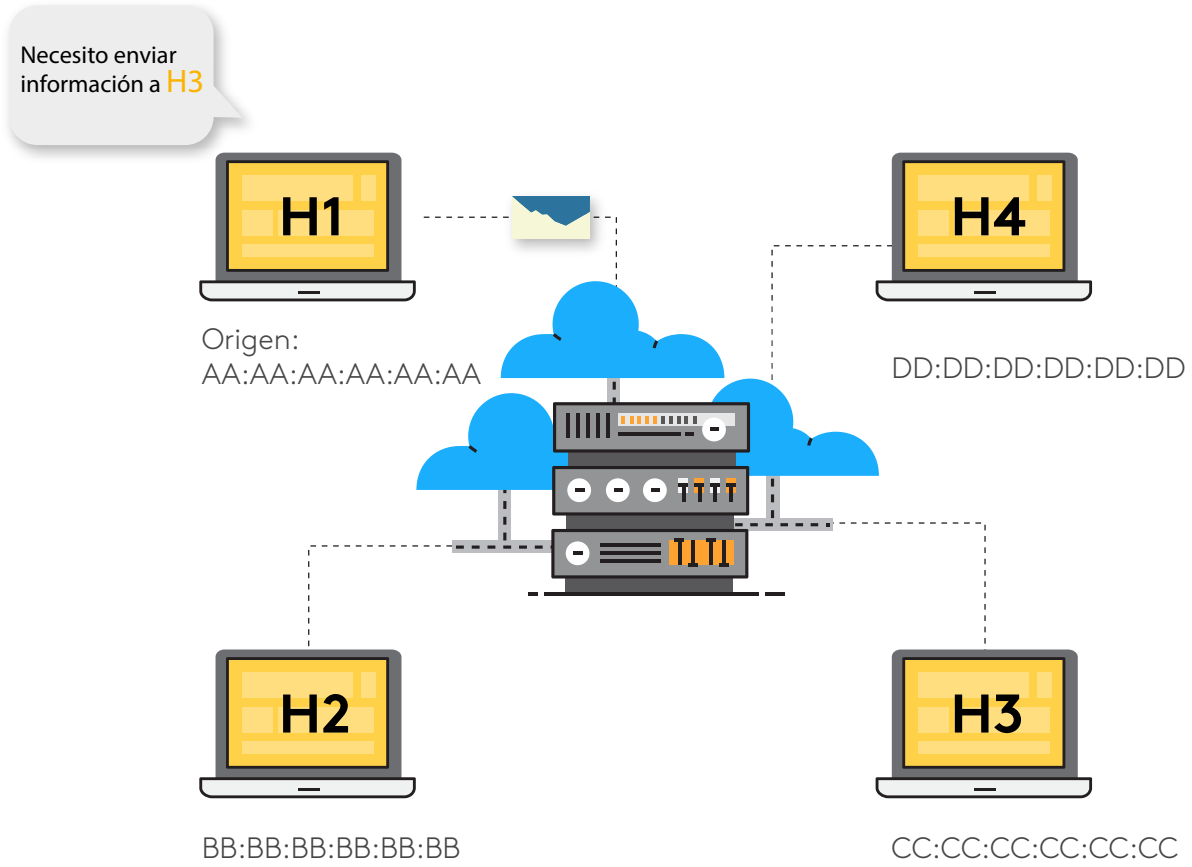


Figura 1.
Fuente: Quintero (2014)

Dentro de la red es necesario conectar dispositivos de origen y destino para que los datos sean transmitidos y poder establecer una comunicación. Esta labor la llevan a cabo los llamados dispositivos intermedios. Se pueden encontrar diversos dispositivos intermedios como: NIC, *hubs, bridge, switches, routers, routers* inalámbricos y *firewalls*. Cabe resaltar que para que exista el intercambio de información necesitamos unos medios de trasmisión, estos pueden guiados (alámbricos) y no guiados (inalámbricos).

Los dispositivos intermedios tienen entre sus objetivos: seleccionar la mejor ruta en la red (*routers*), brindar acceso a los diferentes terminales de la red (*switch*) y garantizar seguridad en la información (*firewall*).

Ejemplo

Ejemplo claro del funcionamiento de estos elementos es una oficina postal o de mensajería. Imagine que usted es el remitente y su jefe el receptor. Lo primero que usted hace es redactar el mensaje y después lo introduce en el sobre. Al marcar el sobre, le coloca los datos del remitente y receptor o destinatario. Sin datos como dirección de origen y destino, código postal, etc., no puede enviar el sobre. Luego, usted procede a llevar el sobre a la oficina postal, donde lo radica con todos los datos mencionados. Inmediatamente, le entregan un desprendible con un radicado, el cual cuenta con un número de referencia. Ahora, usted espera la respuesta al mensaje.

Figura 2. Entrega de sobres en oficina postal
Fuente: Shutterstock/506016142

En este ejemplo podemos relacionar los dispositivos finales e intermedios y su funcionamiento, los cuales analizaremos a continuación.

Adaptadores de red o NIC (*network interface card*)

Antes de profundizar en los dispositivos es importante tener presente cómo los usuarios accedemos a la red. Lo hacemos a través de las NIC, las cuales se encuentran ubicadas en nuestros PC y nos facilitan conectarnos a la red local.

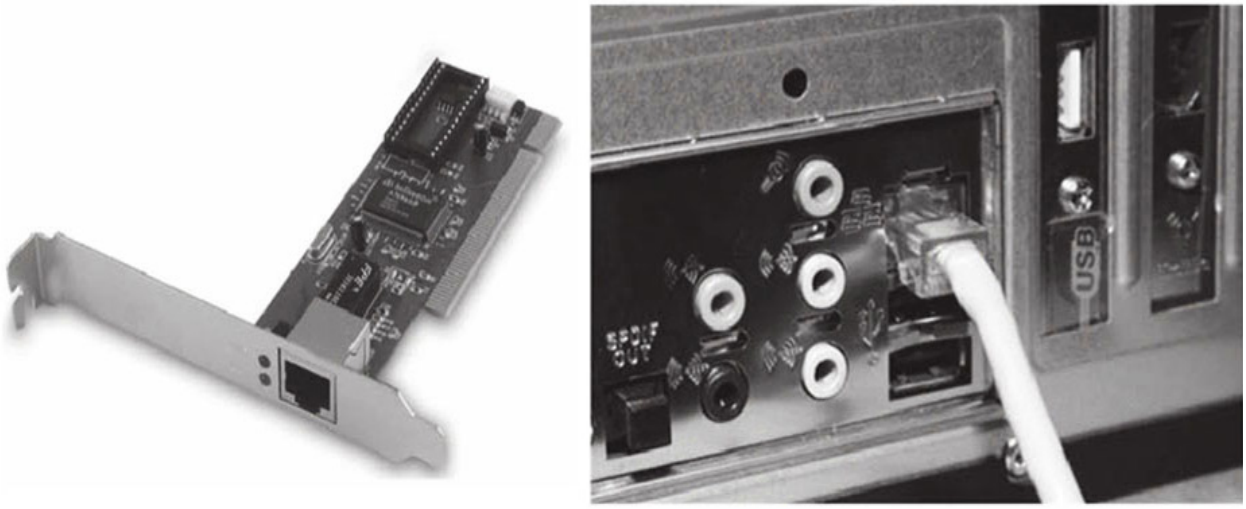


Figura 3.
Fuente: Moreno Pérez (2014)

Características

- La tecnología que manejan estos adaptadores es Ethernet, por lo cual vemos un puerto para conectar la NIC RJ45. Además, tienen una dirección MAC asociada. Esta dirección la podemos apreciar en nuestras PC mediante el comando IPconfig/all dentro del símbolo del sistema. ¿Cómo lo hacemos? Primero vamos a "Inicio", en la opción "Buscar" ingresamos el comando "CMD" seguido de "Enter", inmediatamente ingresamos el comando IPconfig/all y nos arroja nuestra dirección MAC, la cual corresponde a nuestra NIC.

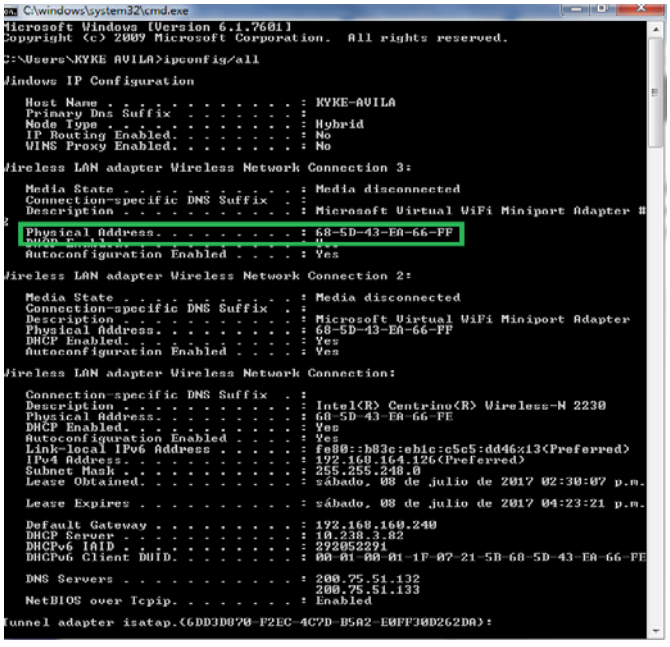


Figura 4.
Fuente: propia

- Las NIC operan en las capas física y enlace de datos del modelo OSI.
- Las tarjetas de red necesitan un controlador o *driver* para que funcionen con el sistema operativo de la PC. Este lo da el fabricante.
- Las NIC pueden encontrarse para conexiones inalámbricas. Estos adaptadores en la actualidad trabajan en las tecnologías como *bluetooth* y wifi. En la figura que veremos a continuación encontraremos una NIC para wifi tipo Pcmcia de Linsys.

Figura 5.
Fuente: Moreno Pérez (2014)

Hubs o concentradores

Son elementos de red Ethernet que permiten conectar varios *hosts* en una red punto a punto.

Características

- Pueden tener en su configuración desde cuatro hasta 32 puertos mediante conector RJ45.
- Trabajan en la capa física del modelo OSI.
- Ventaja: no requieren de una configuración previa, lo cual quiere decir que solamente se dedican a repetir una señal de entrada.
- Desventaja: al enviar mensajes al tiempo se produce una colisión, lo cual causa pérdidas en tiempo real debido a que los mensajes no podrán ser decodificados.
- ¿Qué opinan con relación al ancho de banda? Esta sería otra desventaja porque es-

taríamos manejando el mismo ancho de banda, dado que los dispositivos finales compartirían el canal a la hora del envío y recepción de los mensajes.

- En un tiempo, las topologías estrellas utilizaban estos elementos, después fueron reemplazados por *switches*.

A continuación, se aprecia del HUB 3com SuperStack II Dual Speed Hub 500 24-Port.

Figura 6.
Fuente: https://www.cnet.com/products/3com-superstack-ii-dual-speed-hub-500-24-port/specs/

Puente o bridge

Este dispositivo cuenta con conectores de diferentes tecnologías, lo cual le permite establecer comunicación con redes distintas.

Características

- Tiene semejanza con una estación corriente en la capa de enlace de datos del modelo OSI.

- Si realizamos una analogía con los hubs, los puentes solo permiten el tráfico de un host A instalado en la subred A hacia un host ubicado en la subred B, pero que esté destinado hacia esa subred B. Esta particularidad del puente se conoce como filtro. Esta característica se procesa debido al conocimiento de las dos subredes, dado que ambas están conectadas al puente. En caso de que el puente no identifique al destinatario inundará los demás puertos, ignorando el que le dio el mensaje.

Subred

Término que se asocia a redes secundarias de una red existente.

Figura 7.
Fuente: http://www.produktinfo.conrad.com/datenblaetter/00000-24999/001092789-an-01-es-LINKSYS_WES610N_4PT_DB_BRIDGE.pdf

A continuación, se aprecia el puente Linksys WES610N/WET610N, el cual tiene la capacidad de conectar dispositivos con tecnología Ethernet a la red inalámbrica.

- Un puente permite un mayor rendimiento en cuanto a las conexiones que se pueden implementar en varias redes. ¿Cómo se produce esto? Enfoquémonos en el siguiente ejemplo: tenemos que diseñar una red LAN con 700 *hosts*. Podemos dividir esta LAN en dos subredes mediante un puente, cada subred con 350 *hosts*. Con esto se garantiza optimizar la congestión y, por supuesto, el tráfico.

- Los puentes hoy en día, con la aparición de los conmutadores, muy poco se tienen en cuenta, debido a que los *switches* presentan mayor número de puertos y velocidad en cada uno de ellos.

Conmutadores o *switches*

Los *switches* son dispositivos llamados *switches* LAN. Estos proporcionan conexiones a varios segmentos en una red de área local de manera física a redes más complejas. ¿Qué creen ustedes que sucede al introducir un conmutador por primera vez a la red? Al introducirse en una red, los conmutadores no tienen conocimiento sobre los *hosts* que están conectados en los diferentes puertos, debido a esto se origina una difusión (*broadcast*) hacia estos dispositivos, lo que le permite al conmutador aprender las direcciones MAC de los *hosts* donde se originan los mensajes y armar su tabla de enrutamiento. El proceso de los conmutadores no acaba aún, el *host* al cual va destinado el mensaje recibe dicho mensaje y, automáticamente, da una respuesta al *host* que intenta comunicarse con él, en este caso, el *host* emisor. Cuando se da este proceso de envío y recepción del mensaje a través de los *hosts*, el conmutador podrá indagar sobre direcciones (IP o MAC) de fuente o de origen de los mensajes de respuesta, lo cual le brinda la posibilidad de identificar en qué puertos están conectados estos *hosts* de destino. Una vez el conmutador esté en operación, se genera una tabla dentro de él, en la cual se alojará información pertinente sobre los *hosts* que están conectados por los diferentes puertos.

Conmutador

Elemento que permite la conexión de diferentes equipos dentro de las redes. Un conmutador puede conectar varios dispositivos a la vez que segmentos dentro de las redes, con el objetivo de establecer comunicación entre un host de origen y un host al cual está destinado el mensaje.

Difusión

Hace referencia al hecho de propagar los mensajes a todos los hosts conectados a la red.

Características

- Presentan en su configuración un número de puertos determinados (4, 8, 24, etc.).
- Se desempeñan en la capa de enlace de datos del modelo OSI.
- Con los conmutadores se tiene un mayor rendimiento de la red, debido a que se entra en detalle a mirar cuál es el mensaje de origen y hacia dónde va dirigido. En contexto, se reducen las colisiones.
- Unos de los *switches* que están a la vanguardia es el Cisco Catalyst WS-C2960X-24PSQ-L (Cool). En la figura podrán apreciar este conmutador.

Figura 8.
Fuente: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/data_sheet_c78-728232.html

Se trata de un conmutador de 24 puertos de 10M/100M/1000M que puede alimentar hasta ocho puertos de PoE (los primeros ocho puertos solamente) con capacidad para entregar una suma total de 110W de potencia PoE. Este conmutador tiene cuatro enlaces ascendentes Gigabit Ethernet: dos de ellos SFP y los otros dos interfaces de cobre de 10M/100M/1000M, que permiten elegir la conectividad de fibra o cobre al punto de agregación. Otras características son:

- Se maneja en la capa de enlace de datos del modelo OSI.
- Tiene calidad del servicio. QoS avanzada.
- Seguridad, disponibilidad, escalabilidad y administración avanzadas.
- Rendimiento básico.

Encaminador o *router*

Ahora analicemos el encaminador o *router*, el dispositivo de interconexión con mayor grado de relevancia en las redes informáticas. Este dispositivo es capaz de interconectar redes ubicadas en el mismo nivel o en niveles diferentes. Ejemplo: puede conectar redes que se encuentren en la misma capa de red del modelo OSI o conectar redes que se encuentren en la capa de enlace de datos con la capa de red. Así, el *router* se desenvuelve en la capa de red del modelo OSI (capa 3).

Características

- Como el *router* se maneja en la capa de red del modelo OSI, su función principal es encaminar los paquetes que llegan dirigidos a él hacia el destino correspondiente, siempre con la facultad de distinguir la ruta adecuada o el mejor camino. Este proceso en redes informáticas se conoce como *routing*.

Protocolos

Se entienden como protocolo las normas que manejan los administradores de red para poder establecer comunicaciones efectivas dentro de las redes.

- Los *routers* trabajan de la mano con los protocolos de la capa de red del modelo OSI IPv4-IPv6.

- Los *routers* son optimizadores de recursos, debido a que facilitan la comunicación de cualquier ***host*** con otro *host* a nivel global, regulando el tráfico de información.

- La complejidad de los procesos que realiza como, por ejemplo, decidir cuál es la mejor ruta, enviar mensajes, informar cambios en la red, etc., permite que el *router* tenga un comportamiento como el de un computador. Por esto, dentro del *router* podemos encontrar elementos como:

- Unidad central de proceso (CPU): su función principal es ejecutar las instrucciones del sistema operativo (SO), como la inicialización. Además, tiene funciones de enrutamiento y conmutación.

- Sistema operativo (SO): intérprete entre la máquina y los demás *softwares*.

- Sistemas básicos de entrada y salida (BIOS): permiten el arranque de los ordenadores. Son parte de la ROM.

- Memoria *flash* (no volátil): permite el almacenamiento permanente para el IOS y otros archivos que tienen relación directa con el sistema.

- Memoria RAM (*random access memory*): almacena aplicaciones y procesos, como Cisco IOS, archivo de configuración en ejecución, tabla de enrutamiento IP y caché ARP.

- Memoria Nvram (memoria de acceso aleatorio no volátil): permite el almacenamiento permanente para el archivo de configuración de inicio (startup-config). Esta característica permite que no se pierda la información una vez se apaga el *router*.

- Memoria ROM (*read only memory*): consiste en un *firmware* incorporado en un circuito integrado en los enruta-

dores, con la propiedad de que al apagar este dispositivo no se pierde el contenido en los *routers*. La memoria ROM permite almacenar instrucciones de arranque, *software* de diagnóstico básico e IOS limitado.

En la siguiente imagen veremos *routers* que en la actualidad está enfocando Cisco para sucursales en donde proporcionará características como: virtualización, colaboración multimedia y ahorro de costos en las operaciones. Nos referimos a Cisco 1941 y Cisco 1941W. Estos ofrecen la integración del punto de acceso IEEE 802.11n y se conocen como dispositivos multipropósito (funcionan como *router, switch* y AP).

Virtualización

Hace referencia al uso de la tecnología de una manera que se pueden usar los recursos en cualquier momento y lugar de manera online. Ejemplo: hoy en día servidores virtuales, o sea, en la nube, son los que resguardan nuestra información.

Figura 9.
Fuente: http://www.cisco.com/c/en/us/products/collateral/routers/1900-series-integrated-services-routers-isr/data_sheet_c78_556319.html?dtid=osscdc000283

Puntos de acceso inalámbrico

Hoy en día, la mayoría de las empresas adoptan tecnologías que garanticen buena comunicación, buen rendimiento y que estén al alcance de sus bolsillos. Por estas razones, encontramos dispositivos como los puntos de acceso inalámbrico.

Características

- Tienen un radio de operaciones para su funcionamiento, debido a que no tienen estipulados cables en sus conexiones de red.
- Dan practicidad a la hora de que los usuarios dentro de la red accedan a dicha red de manera inalámbrica sin perturbaciones.
- Dependiendo del radio al cual se van a someter los puntos de acceso, se hace necesario saber la potencia para que el rendimiento sea el adecuado. La conexión entre varios puntos de acceso se logra a través de

medios guiados y no guiados. Con esta descripción surge la pregunta: ¿qué medios utiliza una antena de tecnología móvil y cuáles medios utiliza un punto de acceso dentro de una organización, por ejemplo, dentro de una biblioteca? Las antenas de tecnología móvil se comunican entre sí por enlaces concatenados de microondas o mediante cables. Ahora, los puntos de acceso en una red informática dentro de una biblioteca se interconectan con medios guiados RJ45.

Medios guiados

Son aquellos que necesitan un medio físico. Ejemplo: fibra óptica para la transmisión de las señales.

En la figura veremos un punto de acceso UniFi AP-Outdoor+ (UAP-Outdoor+) que ofrece wifi con una tecnología MIMO 802.11n para un rendimiento superior en las bandas de 2,4 o 5 GHz y alcanza hasta 600 pies.

Figura 10.
Fuente: https://dl.ubnt.com/datasheets/unifi/UniFi_AP_DS.pdf

Dispositivos multipropósito

Muchas veces el usuario desea encontrar dispositivos que le permitan realizar o integrar todas las funciones en un solo dispositivo. Hoy, en el mercado podemos encontrar dispositivos multipropósitos, esto se evidencia en el sector hogar, en donde el usuario prefiere tener dispositivos multipropósito con cada una de las funciones que realizan un *switch*, un punto de acceso inalámbrico y un *router*.

En la siguiente figura se puede visualizar el "Linksys WAP300N". En el *link* pueden apreciar que es un dispositivo multipropósito que cuenta con cuatro modos de uso en su forma de operar: el primero es modo punto de acceso (por defecto), después nos encontramos con el modo *wireless media connector* (conector de medios inalámbricos), seguido a este nos encontramos con el modo *wireless range extender* (amplificador de rango inalámbrico) y, por último, opera en el modo *wireless bridge* (puente inalámbrico).

Figura 11.
Fuente: http://www.linksys.com/co/support-article?articleNum=136121

Factores de forma del *switch*

Uno de los temas que determinan un buen diseño y una posterior configuración de redes informáticas es la correcta elección de los elementos o dispositivos. En este apartado nos enfocaremos en los factores de forma del *switch*. Este término lo podemos asociar como un patrón de medida a la hora de la elección de estos, dado que, dependiendo de la forma, el tamaño, la posterior ubicación en el *rack*, la configuración, ya sea fija, modular, apilable o no apilable, se puede determinar cuál *switch* es el adecuado en nuestras redes.

Analicemos el comportamiento de los *switches*, según su configuración:

- ***Switches* de configuración fija:** estos se basan en la configuración y las características que vienen preestablecidas por parte del fabricante, con lo cual podemos determinar que no se permite implementar cambios. Ejemplo: al tener en nuestra red un *switch* que contempla N números de puertos es imposible agregar más puertos a nuestro *switch*.

  Ejemplo de un *switch* de configuración fija es el EX2200 de Juniper. En la siguiente figura se puede apreciar y en el *link* se encuentra la descripción.

Figura 12.
Fuente: http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000307-en.pdf

- ***Switches* de configuración modular:** pueden llegar a tener más de 1000 puertos en su fisionomía, dado que en su chasis pueden presentar módulos para la inserción de nuevas tarjetas con un determinado número de puertos. Estos *switches* los utilizan las grandes compañías y los ISP. Debido a estas configuraciones podemos decir que estos conmutadores modulares se pueden amoldar a las necesidades futuras de las diferentes redes informáticas dentro de las organizaciones. En las empresas donde el número de clientes crece considerablemente en el tiempo esta característica se conoce como escalabilidad.

  Un ejemplo de un *switch* de configuración modular es el Conmutador HPE FlexFabric Serie 12900. En la siguiente figura se puede apreciar y en el *link* se encuentra la descripción.

Figura 13.
Fuente: https://www.hpe.com/lamerica/es/productcatalog/networking/networking-switches/pip.hpe-flexfabric-12900-switch-series.5443167.html

- ***Switches* de configuración apilable:** poseen un cable en la parte trasera que se denomina *backplane*, el cual tiene la característica de interconectar varios *switches*. De esta manera, facilita la obtención de un número mayor de puertos al unir los diferentes *switches*, lo cual es determinante al momento de ahorrar recursos dentro de las organizaciones, permite un manejo práctico en cuanto al rendimiento (ancho de banda) y posibilita la escalabilidad.

  Un ejemplo de un *switch* de configuración apilable es el ERS 5000. En la siguiente figura se puede apreciar y en el *link* se encuentra la descripción.

Figura 14.
Fuente: https://www.avaya.com/es/documents/ethernet-routing-*switch*-serie-5000-de-avaya-dn5098sp.pdf?t=0

¿Qué son las redes conmutadas?

Hace años surgió la arquitectura LAN más común: Ethernet 802.3. Esta tecnología de conmutación se caracterizaba por enviar datos dentro de la red a los diferentes dispositivos. Se basaba en topologías bus, las cuales advierten muchos inconvenientes al momento de implementarlas. Ejemplos de estos inconvenientes son:

LAN

(Local area network): son redes de área local utilizadas por los administradores en la mayoría de las organizaciones.

- Después de 500 m es necesario utilizar repetidores, debido a que la señal se debilita. A esto se le suman los factores atmosféricos.
- La implementación de los recursos es elevada.
- Al momento de presentarse una caída de uno de los ***hosts*** se interrumpe la comunicación en toda la red.
- Se debe compartir el ancho de banda (10 Mbps), por lo cual se producen muchas colisiones y retardos en la red.

Al incorporar dispositivos de capa 2, como los conmutadores, no ocurren inconvenientes como los expresados; por ejemplo: "Al momento de presentarse una caída en uno de los ***hosts*** se interrumpe la comunicación en toda la red", debido a que los conmutadores tienen la capacidad de aprender las direcciones MAC ubicadas en las tramas transmitidas. Gracias a esta característica, toman decisiones acerca del reenvío de mensajes, lo cual alivia las colisiones dentro de la red. Los conmutadores envían mensajes de difusión a los dispositivos que forman parte de la red, produciendo un bajo rendimiento de esta. Al sumar dispositivos de capa 3, los ***routers***, estos cumplen un papel fundamental a la hora de escoger el mejor camino de envío y recepción de los mensajes. Con los ***routers*** no se manejan tráficos por difusión, lo cual aumenta el rendimiento de las redes LAN.

Los administradores de red implementan en su diseño dispositivos de interconexión en las diferentes capas del modelo OSI (física-enlace de datos-red). Esto se hace partiendo de las prioridades en las redes LAN. En su desarrollo, las LAN empezaron a sufrir congestión y retardos en sus actividades, debido al gran consumo de ancho de banda en los servicios que se manejaban dentro de estas: telefonía convencional, PC de escritorio, impresoras, escáner, portátiles, tabletas, transferencia de archivos, transacciones, videos, mensajería, etc. Por esta razón, hoy tenemos tecnologías más avanzadas como las LAN conmutadas, que permiten un mayor ancho de banda dentro de las organizaciones, lo cual mejora el tráfico y da un mayor rendimiento a las LAN. Esto se logra con la utilización del ancho de banda por cada usuario sin interferir con el resto de la red. Se puede decir que se tiene un ancho de banda dedicado a los diferentes usuarios.

Características de las LAN conmutadas

- Los dispositivos de las LAN conmutadas deben tener la propiedad de convivir con tecnologías existentes y, además, de acoplarse a los cambios que se presentan a diario en la tecnología (por ejemplo, VOIP). Para entrar en contexto, la telefonía análoga debe ser aceptada y propiciada en las redes conmutadas.

- Se maneja calidad del servicio (QoS).
- Al manejar cantidades de información, es importante garantizar que dicha información sea protegida. Esto implica tener un alto grado de seguridad en las redes LAN dentro de las organizaciones.
- Las redes conmutadas tienen como principio converger tecnológicamente. Esto va de la mano con lo que se conoce hoy en día como redes convergentes.

QoS

Del inglés quality of service, hace referencia a la calidad del servicio; por ejemplo, al administrar el ancho de banda dentro de una organización debemos dar prioridad a servicios como las llamadas telefónicas y la transferencia de archivos; y una reducida parte del ancho de banda al video, dado que este consume mucho.

Redes convergentes

La mejor manera de interpretar las redes convergentes es comprender la necesidad que tienen los diferentes organismos de llevar cada uno de los servicios, como voz, datos y video, por un solo medio. Un ejemplo son los operadores que tenemos en Colombia, como Claro, los cuales nos entregan por un mismo medio tecnología coaxial, HFC (híbrido de fibra y coaxial) o fibra óptica, servicios de TV, telefonía e internet, con la particularidad de un "reuso" de la señal. Esto indica que, en horas esenciales para el descanso del colombiano, puede ser a las 8:00 p. m., hay una lentitud al acceso de la red, debido a que la tecnología, en este caso de fibra, sale de la estación principal y llega a los diferentes nodos y de ahí se redistribuye la señal a los abonados vinculados a dicho nodo.

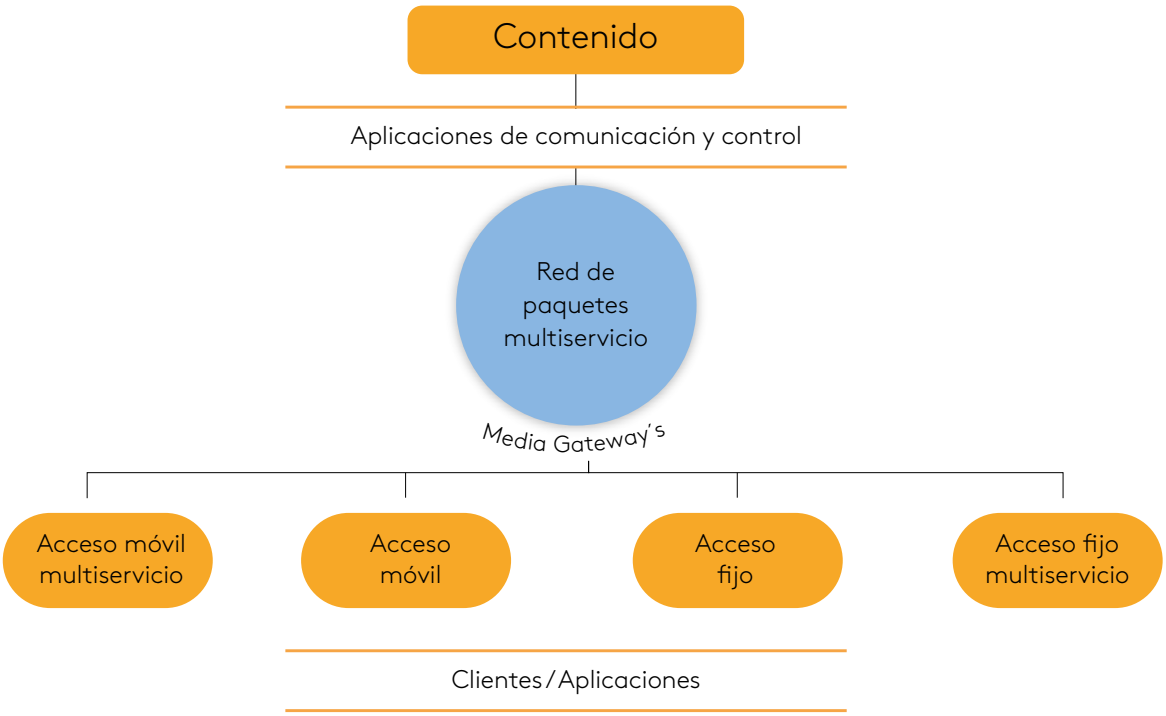


Figura 15.
Fuente: https://www.crcom.gov.co/recursos_user/Actividades%20Regulatiorias/regulacion_redes/Unicauca.pdf

Características

- Las redes convergentes implementan en su configuración y diseño una única red física indispensable para garantizar eficacia al momento de administrar las redes informáticas.

- La implementación del protocolo IP dentro de cada uno de los servicios que se prestan en las redes: voz, datos y video, idealizando una red donde el tráfico y el transporte confluyen sobre una red que converge. Con este uso de IP en las redes convergentes se obtiene lo siguiente:

  - Los administradores de red tendrán un manejo apropiado en la administración de la red.

  - Una mejor distribución del ancho de banda dentro de las organizaciones para optimizar recursos.

  - Capacidad de adoptar nuevas aplicaciones dentro de las empresas.

- En las organizaciones podemos encontrar tecnologías que permiten un manejo práctico de las llamadas. Un ejemplo de esto es la posibilidad de tener oficinas con teléfonos IP, los cuales brindan opciones como: si usted no se encuentra en su punto de trabajo y entra una llamada, el teléfono inmediatamente identifica la llamada y puede transferirla. Además, si estamos ocupados cuando entra la llamada, podemos usar la llamada en espera; asimismo, frente a una reunión con socios o clientes, podemos realizar una teleconferencia.

- A través de las redes convergentes podemos implementar la mensajería, mediante voz o datos, incluyendo multimedia.

- Con el advenimiento de los *smartphones* podemos establecer una comunicación en tiempo real a cualquier hora del día y en cualquier lugar del planeta.

¿Qué es Cisco Borderless Network?

Imaginemos el siguiente escenario: una red Campus que establece comunicación con sus dos sucursales dentro de la ciudad de Barranquilla. En cada una de ellas hay un servidor y servicios de voz y datos. Además, estas sucursales tienen acceso a internet, cuentan con la telefonía tradicional PSTN y acceso a internet inalámbrico. Para conseguir el correcto funcionamiento en las sucursales de la red convergente es fundamental la implementación de una arquitectura que se conoce como Cisco Borderless Network. Esta tecnología incluye en su puesta en marcha una inteligencia en torno a la aceptación de futuros usuarios en las sucursales, esta característica se denomina escalabilidad.

PSTN

Del inglés public switched telephone network (red de telefonía pública conmutada), es una red de telecomunicaciones en donde se dan las comunicaciones mediante líneas telefónicas en tiempo real.

Con Cisco Borderless Network tenemos redes sin fronteras. Analicemos esa frase: "redes sin fronteras", inmediatamente se nos viene a la mente que no hay límites, que nos podemos comunicar, relacionarnos con determinado número de personas, organizaciones, etc., a cualquier hora del día independiente del lugar en que nos encontremos. Aún mejor, podemos lograr una interacción en los entornos donde nos

encontremos para propiciar la mejor manera de laborar y establecer negocios alrededor del mundo.

Las redes convergentes sin fronteras nos indican que los procesos deben realizarse con normas, lineamientos o doctrinas adecuados. Partiendo de este parámetro, las redes convergentes necesitan guiarse por un modelo en capas o diseño jerárquico que garantice un manejo apropiado de la información.

Modelo jerárquico de las redes convergentes

En la siguiente figura podemos apreciar el modelo jerárquico de las redes convergentes y sus capas.

Algunas características del modelo son:

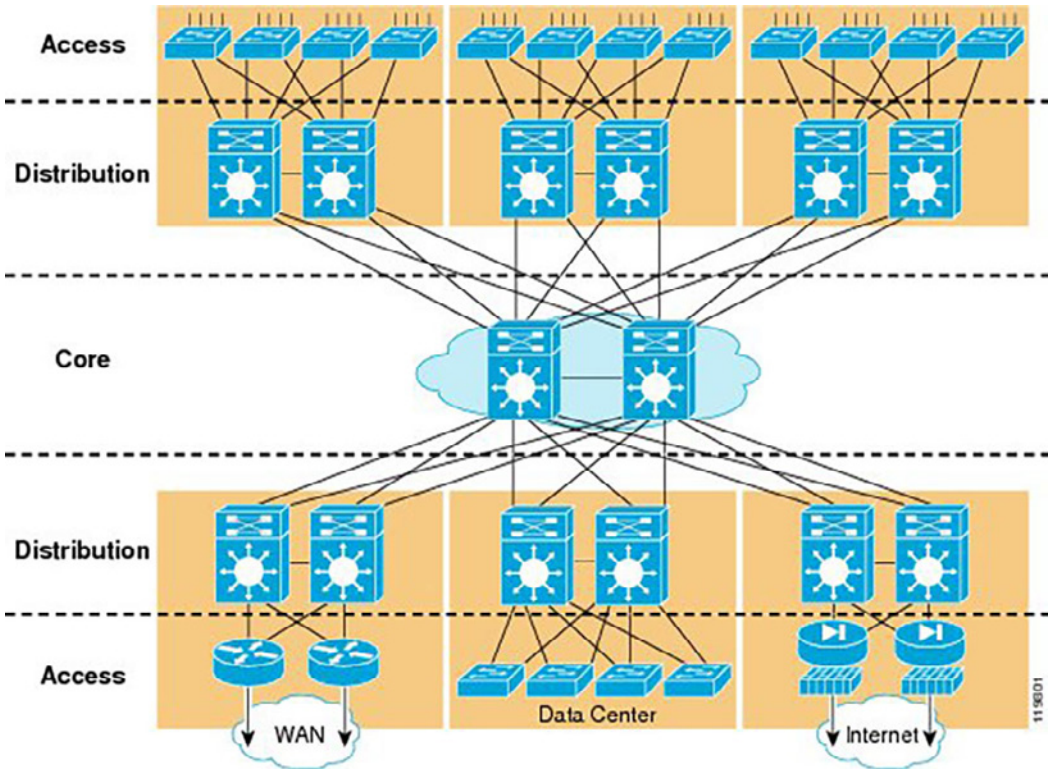


Figura 16.
Fuente: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/ha-campusdg.html?dtid=osscdc000283

- Brinda garantías en la confiabilidad al pensar en un diseño de redes conmutadas sin fronteras, basándose en establecer una jerarquía. Sin esta, no se podría identificar el rol de los diferentes elementos y dispositivos dentro de las redes.

- Un buen diseño debe aceptar evolución y crecimiento. Debe contemplar la idea de incorporar nuevos usuarios a las redes, lo cual se comprende como la capacidad de ser modular.

- Al presentarse alguna falla dentro de la red, esta debe ser inteligente para garantizar su funcionamiento. Esto se conoce como capacidad de recuperación.

- ¿Qué tan segura es nuestra red al brindar acceso a un socio en una reunión? Partiendo de la premisa de que la información es lo más importante para las organizaciones, debemos garantizar que nuestro socio tenga acceso a internet, pero con limitaciones. Si una persona no autorizada se conecta a nuestra red con intenciones maliciosas, debemos estar en capacidad de denegar este acceso por medio de políticas y bloquearla.

Capas del diseño jerárquico de redes

1. **Capa de acceso:** facilita que los usuarios o dispositivos finales accedan a la red. Estos tienen la característica de estar conectados a *switches* de acceso que, a su vez están conectados a los *switches* de la capa de distribución. Ejemplo: los *switches* catalyst 2960 de Cisco. Hoy en día la eficiencia y la seguridad de estos *switches* facilitan la administración de las diferentes aplicaciones. Debido a la inteligencia que poseen estos dispositivos, en esta capa se pueden agregar más enlaces.

2. **Capa de distribución:** favorece la interoperabilidad entre las capas de acceso y ***core*** del modelo jerárquico. Facilita enlaces redundantes para garantizar el funcionamiento de la red. Además, en su funcionamiento, implementa conmutadores de capa 3; por ejemplo: el *switch* catalyst 3750 de Cisco capa 3 maneja QoS.

3. **Capa de núcleo o *core*:** es la capa central de la red. En esta se manejan muchas velocidades. Por la gran cantidad de información que se trata, se garantiza QoS. Esta capa implementa *switches* modulares; por ejemplo, el *switch* catalyst 6500 de Cisco.

BIBLIOGRAFÍA

Aznar López, A. (2005). *La red internet. El modelo TCP/IP*. Madrid, España: Grupo Abantos Formación y Consultoría.

Boronat Seguí, F. (2013). *Direccionamiento e interconexión de redes basadas en TCP/IP: IPv4/IPv6, DHCP, NAT, encaminamiento RIP y OSPF*. Valencia, España: Editorial de la Universidad Politécnica de Valencia.

Carceller Cheza, R. (2013). *Servicios en red*. Madrid, España: Macmillan Iberia S. A.

Castaño Ribes, R. J. (2013). *Redes locales*. Madrid, España: Macmillan Iberia S. A.

Hallberg, B. (2007). *Fundamentos de redes*. Madrid, España: McGraw-Hill Interamericana.

Hillar, G. C. (2004). *Redes: diseño, actualización y reparación*. Buenos Aires, Argentina: Editorial Hispano Americana S. A.

Íñigo Griera, J. (2008). *Estructura de redes de computadores*. Barcelona, España: Editorial UOC.

Jiménez Camacho, R. (2014). *Análisis del mercado de productos de comunicaciones (UF1869)*. Málaga, España: IC Editorial.

Martínez Yelmo, I. (2015). *IPv6-Lab: entorno de laboratorio para la adquisición de competencias relacionadas con IPv6*. Madrid, España: Universidad de Alcalá.

McGraw-Hill Interamericana. (2013). *Redes locales*. Madrid, España: McGraw-Hill.

Molina Robles, F. J. (2014). *Servicios de red e internet*. Madrid, España: RA-MA Editorial.

Moreno Pérez, J. C. (2014). *Sistemas informáticos y redes locales*. Madrid, España: RA-MA Editorial.

Quintero, E. B. (2014). *UF1879: equipos de interconexión y servicios de red*. Málaga, España: IC Editorial.

Santos González, M. (2014). *Diseño de redes telemáticas*. Madrid, España: RA-MA Editorial.

Velte, T. J. (2008). *Manual de Cisco®*. Madrid, España: McGraw-Hill Interamericana.

ENRUTAMIENTO Y CONFIGURACIÓN DE REDES

Ricardo López Bulla

EJE 2

Analicemos la situación

AREANDINA
Fundación Universitaria del Área Andina
MIEMBRO DE LA RED ILUMNO

Fuente: Shutterstock/258980774

INTRODUCCIÓN

Para las organizaciones, las redes informáticas constituyen una herramienta fundamental que parte del establecimiento de relaciones, ya sea con otras organizaciones o con el personal dentro de esta, para desarrollar las actividades enfocadas a mantener procesos efectivos con base en una óptima comunicación, lo cual facilita la buena actuación de dichas organizaciones. Un administrador de red posee la capacidad de diseñar redes informáticas enfocadas en una buena ruta para la correcta transmisión del mensaje; con esto, garantizará el rendimiento y efectividad de la red.

Los ***routers*** son dispositivos que basan su funcionamiento en la adopción del conocimiento, mediante las tablas de enrutamiento. Factores como origen y destino de los mensajes permiten determinar cuáles mecanismos y protocolos tener en cuenta a la hora de configurar y enrutar las redes informáticas. En este eje, se analizará el enrutamiento (estático y dinámico) y los protocolos, así como el funcionamiento y sus características. Además, se encontrarán actividades como lecturas complementarias, videocápsulas e infografías, etc., que lo ayudarán a comprender los temas descritos.

Importancia del enrutamiento

El enrutamiento es un proceso que facilita a elementos o dispositivos de interconexión disponer de la mejor ruta en la emisión y recepción de los mensajes. Esta ruta la podemos obtener mediante el encaminador o router. Con esta doctrina, podemos decir que el enrutamiento basa su funcionamiento en la capa de red del modelo OSI.

Doctrina
Grupo de ideas que se dan en torno a un tema específico.

Filtro
Seleccionar datos para establecer una información.

¿Cómo operan los *routers*?

En el eje 1 se abordó el router y se expusieron sus características. Es importante repasar estos conceptos para tener claro el funcionamiento del encaminador. Sabemos que el *router* es un dispositivo capaz de interconectar redes ubicadas en el mismo nivel o en uno diferente. Ejemplo: puede conectar redes que se encuentren en la misma capa de red del modelo OSI o, por lo contrario, conectar redes que se encuentren en la capa de enlace de datos con la capa de red. Así, el router se desenvuelve en la capa de red del modelo OSI y en las capas por debajo de esta.

- Los *routers* trabajan de la mano con los protocolos de la capa de red del modelo OSI IPv4 (algunos aceptan IPv6).
- Los *routers* son optimizadores de recursos, debido a que facilitan la comunicación de cualquier host con otro *host* a nivel global, regulando el tráfico de información.
- Los *routers* informan constantemente a sus vecinos sobre los cambios que se están presentando dentro de la red.
- Un encaminador se encarga de establecer una especie de filtro, ya que analiza la información y toma decisiones acerca del tráfico no deseable, garantizando cierto grado de seguridad a los usuarios dentro de la red.

En la siguiente figura podemos apreciar la elección de la mejor ruta por parte del *router*.

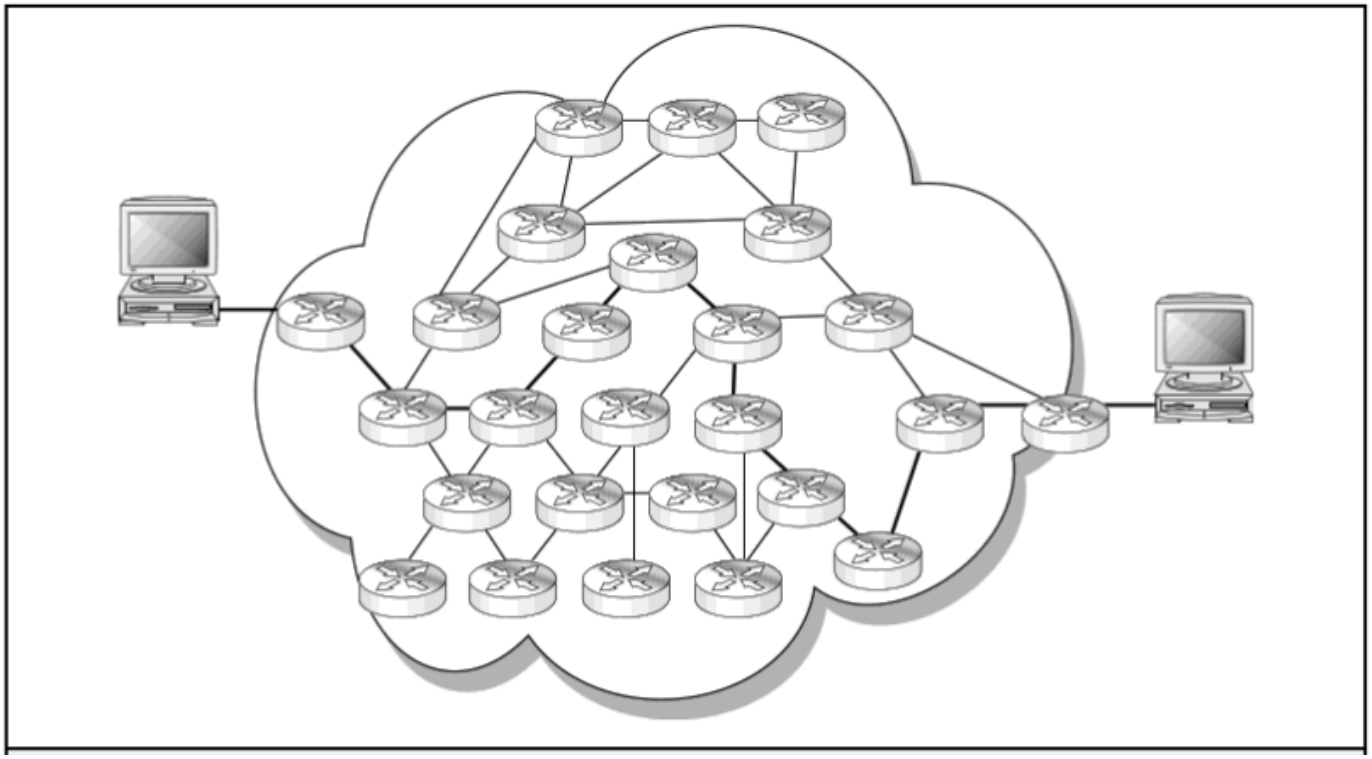


Figura 1. Elección de ruta por parte del *router*
Fuente: Velte (2008)

Elección de la ruta

La escogencia de la mejor ruta por parte de los encaminadores tiene su proceso en la capa de red del modelo OSI, después de un análisis de todas las rutas disponibles en la red informática para dirigir el paquete hacia su destino. Para la elección de la mejor ruta existen factores importantes:

- **Métrica:** es un valor que caracteriza los protocolos de enrutamiento. Mediante este se pueden definir costos, los cuales permiten acceder a redes que se encuentren cercanas. Una métrica de menor tamaño se considera la apropiada.

  - En la siguiente figura podemos apreciar la cantidad de saltos que tiene R1 para llegar a R3, en este caso la métrica es 2.

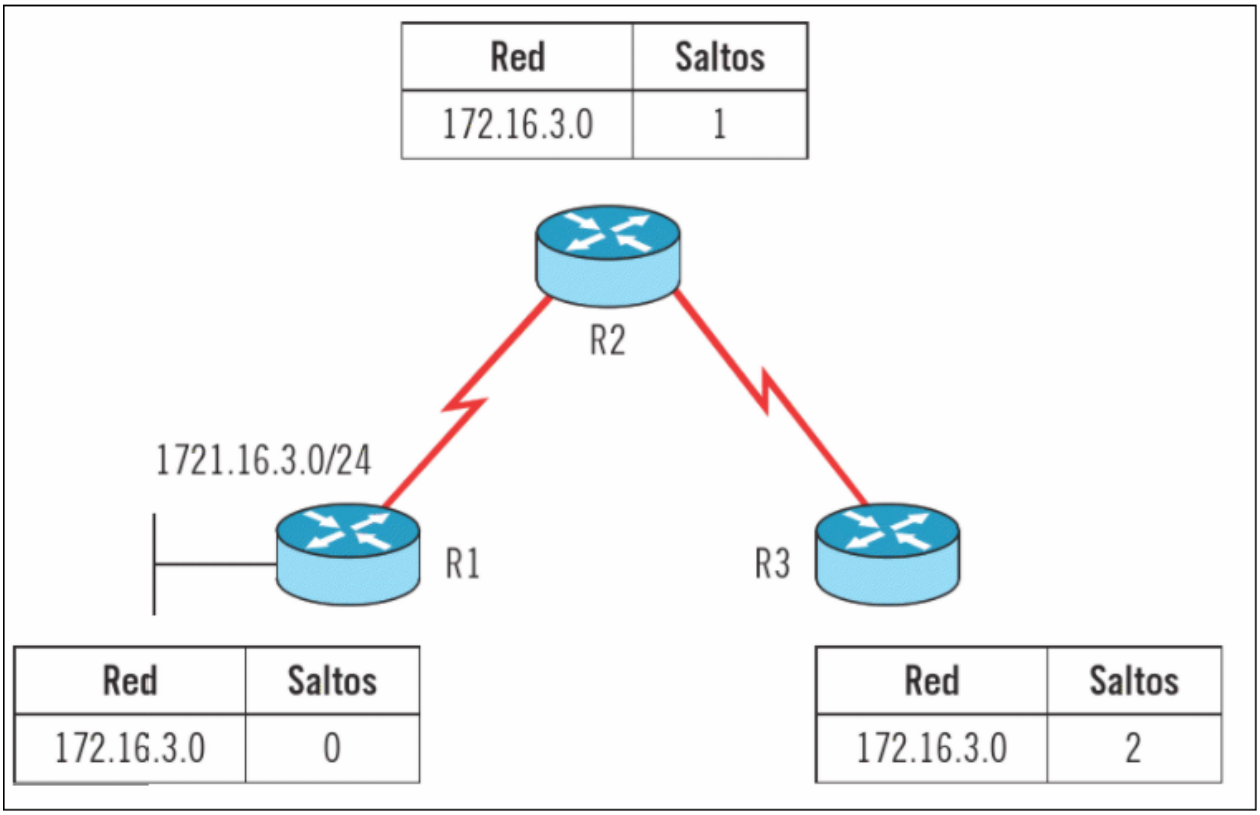


Figura 2. Métrica conteo de saltos
Fuente: Bellido Quintero (2014)

Clases de métricas

- **Costo:** tipo de métrica usada por el protocolo de enrutamiento dinámico OSPF. Este protocolo coloca un precio a cada enlace dentro de la red, enfocado a escoger la mejor ruta.

- **Ancho de banda BW:** permite la elección de la mejor ruta con una preferencia: el mayor ancho de banda.

- **Conteo de saltos (hops):** esta métrica la utiliza el protocolo RIP con un valor de 15. Consiste en contar el número de ***routers*** que tiene que atravesar un paquete para llegar a su destino.

- **Retardo (*delay*):** se comprende como el tiempo que gasta un mensaje desde que sale hasta su destino.

- **Carga (*load*):** se analiza por parte del ***router*** la cantidad o el porcentaje de carga que se encuentra en un enlace para poder decidir cuál ruta escoger, ya que de esta manera se tiene en cuenta aquel enlace que presenta menos congestión.

- **Confiabilidad (*reliability*):** comprende un rango o valor de 0 a 255, en donde el *router* analiza la cantidad de veces que se ha caído un enlace. Se puede deducir que, al tener un menor valor, mayor confianza tiene el ***router*** para enviar por ese camino los paquetes.

- **Distancia administrativa:** este elemento posibilita identificar la ruta que va a ser incluida en la tabla de enrutamiento. La distancia administrativa con un valor inferior tendrá prioridad sobre una de valor superior. Esta relación de valores se hace en torno a protocolos distintos sobre una misma red.

Protocolos
Conjunto de normas y reglas que se deben seguir dentro de un sistema de comunicaciones. Son muy importantes en las redes informáticas, ya que se debe tener el mismo protocolo en las configuraciones al momento de establecer una interconexión.

Origen de la ruta	Distancia administrativa
Conectada	0
Estática	1
Ruta sumarizada EIGRP	5
BGP externo	20
EIGRP interno	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externo	170
BGP interno	200

Tabla 1. Valores de distancias administrativas predeterminadas
Fuente: propia

- **Balanceo de carga:** se origina en el momento en que el ***router*** envía un paquete para el mismo destino por varias rutas. Esto garantiza un balance equitativo en los enlaces.

Análisis de la tabla de enrutamiento

Existe un elemento que distingue la actuación de los *routers* y es la tabla de enrutamiento. Como se sabe, esta tabla la aprenden los *routers* en el proceso de la interconexión con sus vecinos. Brinda la información necesaria en casos específicos, como, por ejemplo, si la red a la cual nos vamos a conectar posee una conexión directa, inmediatamente el encaminador sabe el puerto por el cual se deben enviar los paquetes; en caso contrario, el encaminador nos debe identificar la ruta mediante el procesamiento de datos, obteniendo la mejor ruta para el envío de paquetes. La tabla de enrutamiento es parte vital de los routers para la obtención de información.

Las tablas brindan la información que tienen almacenadas los ***routers*** en la RAM acerca de rutas directamente conectadas y las rutas remotas:

- **Redes directamente conectadas:** tienen prioridad ante las demás redes que se puedan tener dentro de la red. Cada vez que el enrutador crea y activa una interfaz que está directamente conectada se agrega un nuevo camino o ruta.

- **Rutas remotas:** son redes vecinas a una red específica. Para acceder a estas mediante el enrutador, es necesario implementar rutas estáticas o protocolos dinámicos.

En la siguiente figura se puede apreciar una tabla de enrutamiento de Windows. Introduciendo el comando *router print* se visualizan las diferentes entradas de la tabla de rutas IPv4, red de destino, máscara de subred, puerta de enlace, interfaz y métrica.

- ***Network destination***: red a la cual van dirigidos los mensajes.

- ***Netmask***: máscara de la red de destino.

- ***Gateway***: corresponde al identificador del encaminador.

- ***Interface***: dirección mediante la cual se van a enviar los mensajes.

- ***Metric***: valor que caracteriza a los diferentes protocolos de enrutamiento.

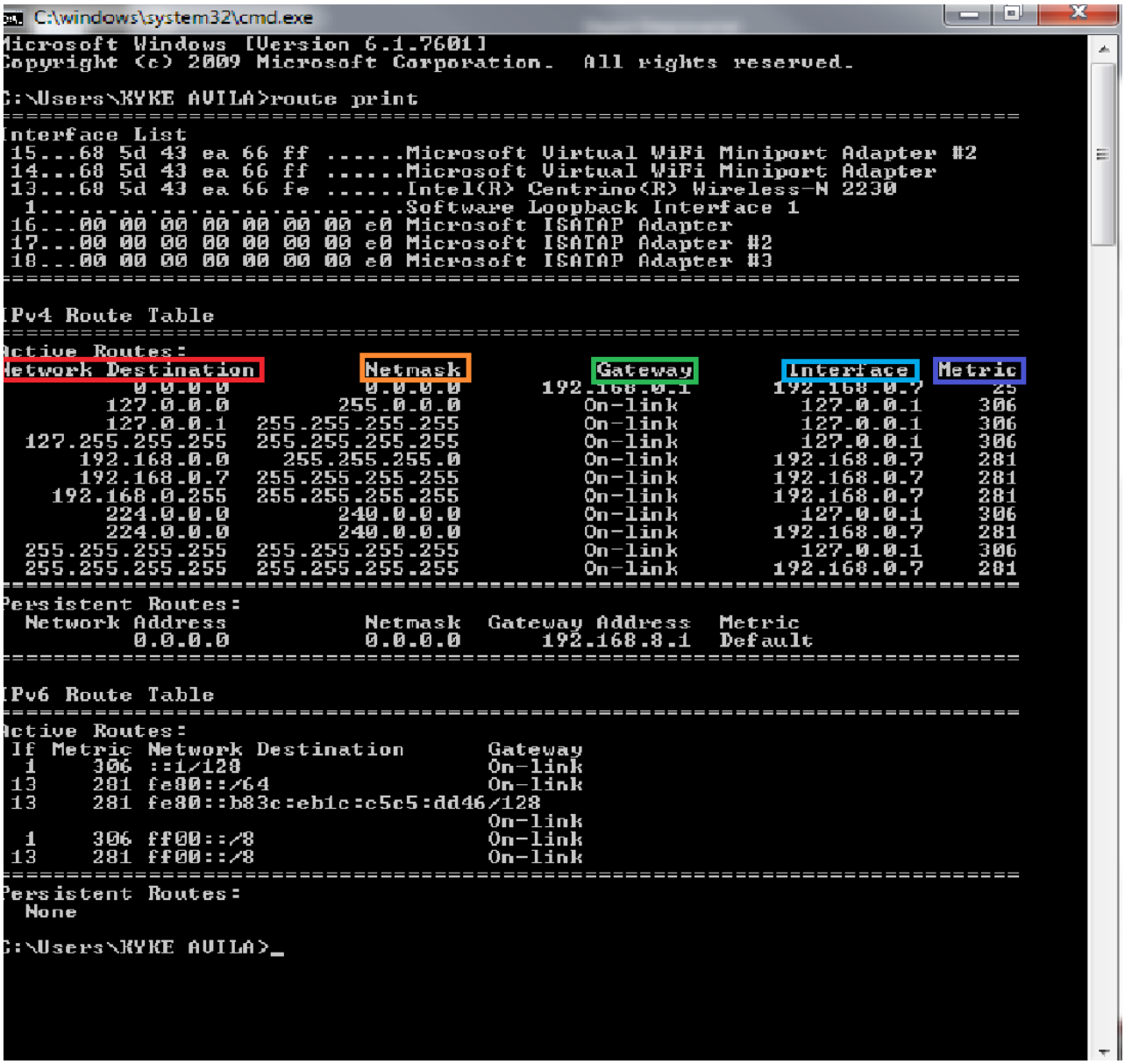


Figura 3. Tabla de enrutamiento de Windows
Fuente: propia

En la próxima figura podemos apreciar el resultado del comando *show ip route* al interior del *router*, mediante el simulador *packet tracer*. Los códigos encerrados en los rectángulos nos facilitan identificar o leer la tabla de enrutamiento para así tener la gestión y el monitoreo ideal en una red informática. A continuación, encontraremos la descripción de estos códigos:

- **L (*local*):** esta es la dirección que identifica al encaminador.
- **C (*connected*):** muestra la red conectada de manera directa al encaminador.
- **S (*static*):** visualiza una ruta creada estáticamente.
- **O (*OSPF*):** advierte que se conoció la ruta de manera dinámica a través del protocolo OSPF.

Los códigos restantes no se abordarán en esta asignatura.

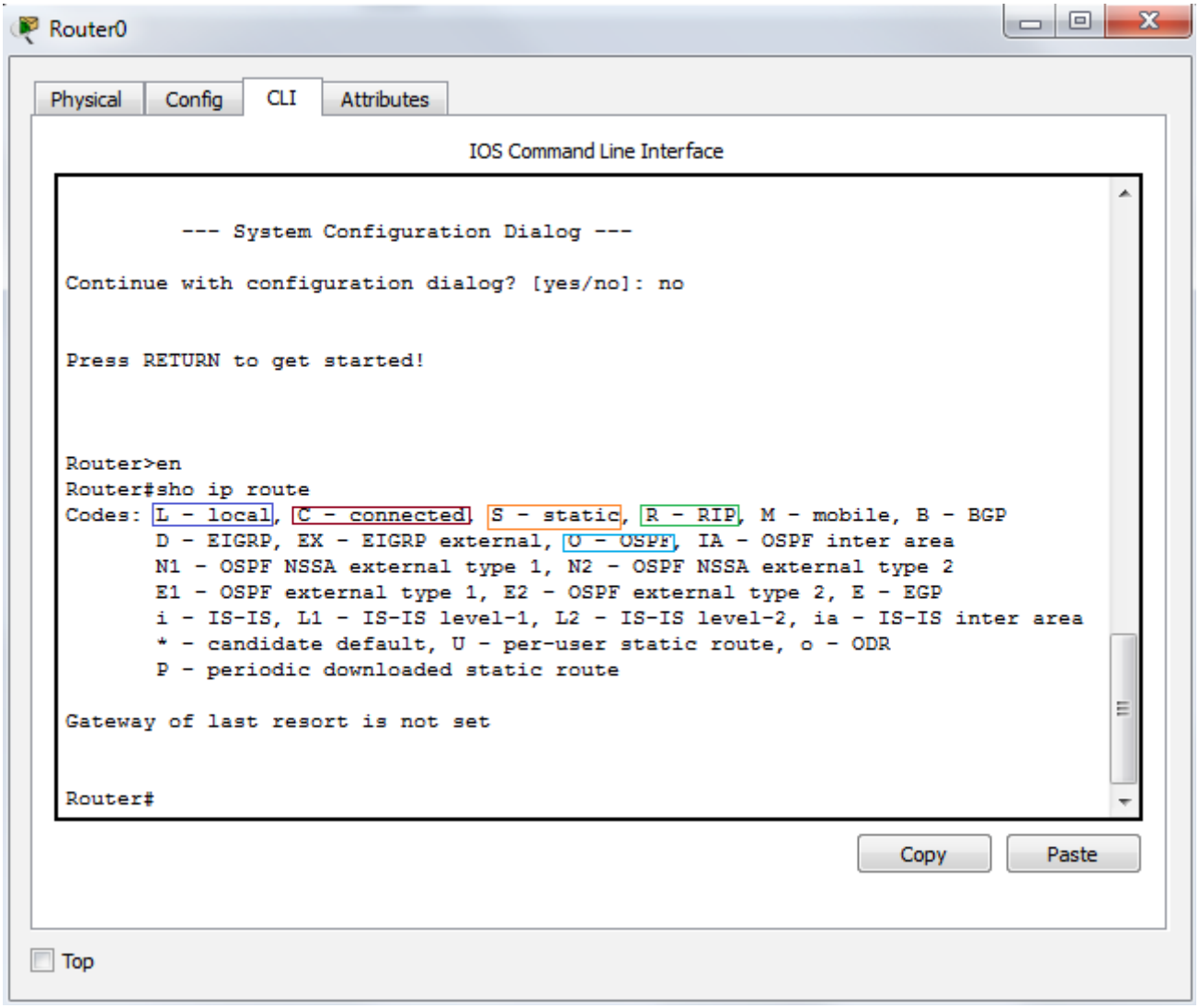


Figura 4.
Fuente: propia

Los *routers* aprenden la tabla de enrutamiento de dos maneras: manual y dinámica.

Enrutamiento estático

Se considera una ruta estática aquella creada manualmente por el administrador de red. Al no tener vínculos con los protocolos, las rutas estáticas no reciben actualizaciones, lo cual indica que el administrador debe reconfigurar estas rutas nuevamente e incluir los cambios en la topología.

Topología
Todos los elementos y la estructura que conforman la red informática.

Ventajas

- Mayor seguridad en las redes informáticas.
- Al no utilizar protocolos de enrutamiento, el consumo de recursos es menor. No se consume mucho ancho de banda.
- Practicidad en la administración por parte del administrador de la red, siempre y cuando la red sea pequeña.

Desventajas

- Al tener cambios en la topología no se presenta una actualización automática.
- Los mantenimientos son complejos.

Tipos

- **Ruta estática estándar:** se enfoca en la conexión de redes cercanas específicas.

  Configuración

  El administrador de red debe asignar el siguiente comando ***ip route***, el cual caracteriza las rutas estáticas. La manera de escribir la línea de comandos para configurar una ruta estática es:

  - **Router (config)#** ip route *{prefijo de red de destino} {máscara} {dirección gateway}*
  - **Router (config)#** ip route *{prefijo de red de destino} {máscara} {interfaz de salida}*

  En el siguiente ejemplo el administrador de red que se encuentra conectado mediante un ***host*** a R1 debe acceder al ***host*** que se encuentra conectado a R2 con la red 192.168.16.0. ¿Qué configuración de enrutamiento estático debe utilizar? El administrador puede acceder al ***host*** ubicado a R2 con los siguientes comandos que corresponden a la dirección del siguiente salto del ***router*** y usando una interfaz:

  - R1(config)# ip route 192.168.16.0 255.255.255.0 192.168.15.1
  - R1(config)# ip route 192.168.16.0 255.255.255.0 S0/0/0

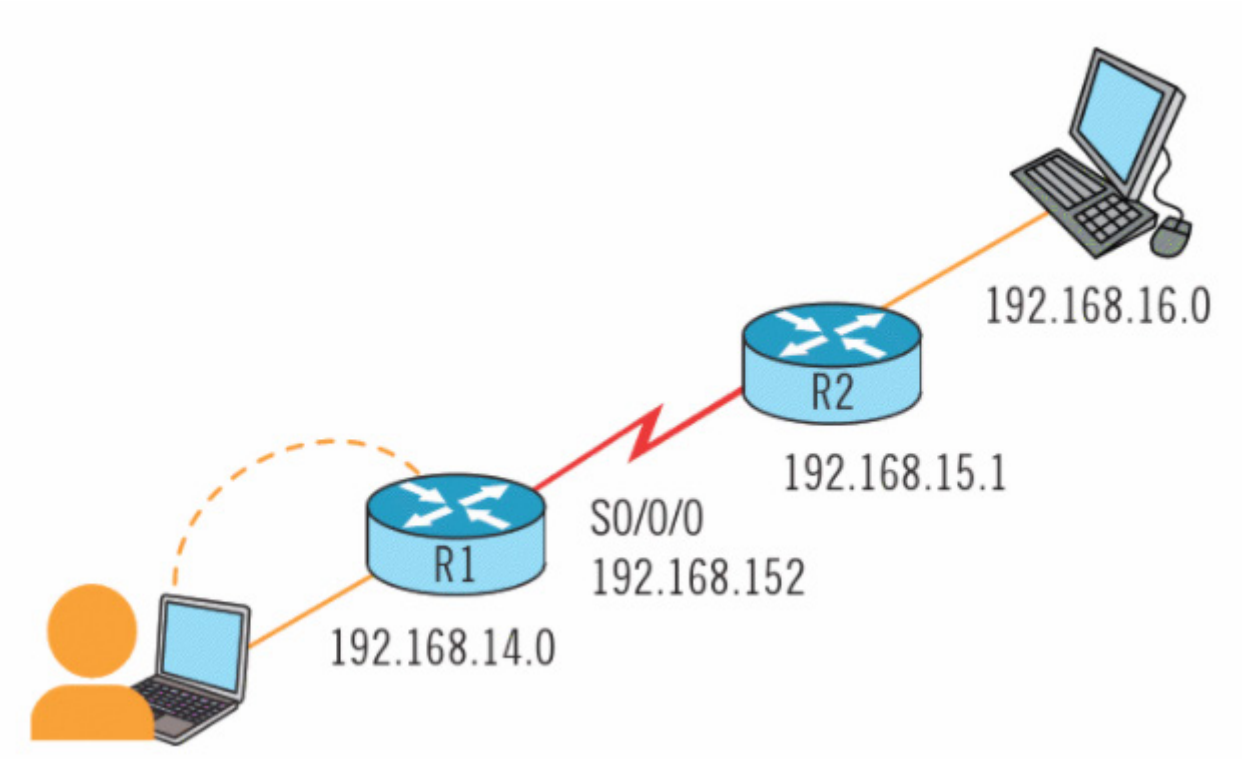


Figura 5. Enrutamiento estático.
Fuente: Bellido Quintero (2014)

- **Ruta estática por defecto:** es muy interesante debido a que encamina todos los paquetes hacia destinos que no cuentan con una referencia en la tabla de enrutamiento. Ejemplo: cuando los proveedores de servicio de internet se conectan con un encaminador adyacente de una multinacional.

Configuración

El administrador de red debe asignar el siguiente comando ***ip route***, el cual caracteriza las rutas estáticas. La manera de escribir la línea de comandos para configurar una ruta estática es:

- ***Router* (config)#** ip route 0.0.0.0 0.0.0.0 *{dirección del siguiente salto}*
- ***Router* (config)#** ip route 0.0.0.0 0.0.0.0 *{interfaz saliente}*

En el siguiente ejemplo, el administrador de red se encuentra una red conectada mediante R1. Este debe acceder a R2, que se encuentra conectado a R2 con la red 192.168.1.0. ¿Qué configuración de enrutamiento estático debe utilizar? El administrador de red puede acceder a R2 desde R1 con los siguientes comandos, que corresponden a la ruta estática por defecto implementando: dirección del siguiente salto del ***router*** y usando una interfaz.

- R1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.5
- R1(config)# ip route 0.0.0.0 0.0.0.0 s0/0/0

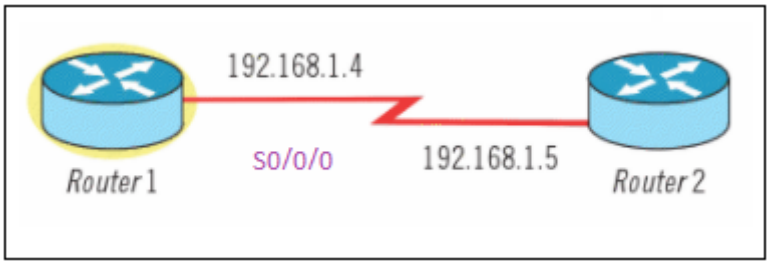


Figura 6. Rutas estáticas por defecto.
Fuente: Bellido Quintero (2014)

- **Ruta estática resumida:** se implementa al momento de encontrarnos en una topología en donde la tabla de enrutamiento es muy grande, debido al establecimiento de conexiones con diferentes rutas estáticas, convirtiéndolas en una sola ruta mediante un proceso de resumen de ruta. Este proceso puede darse si las redes que conforman la topología son adyacentes.

  En la siguiente figura podemos apreciar que *Rcapital* desconoce las redes dentro de la topología; en total son cuatro redes. La manera correcta de acceder a estas redes es realizar un resumen de rutas, ya que todas las redes se encuentran de manera adyacente (192.168.64.0/24 hasta 192.168.67.0/24).

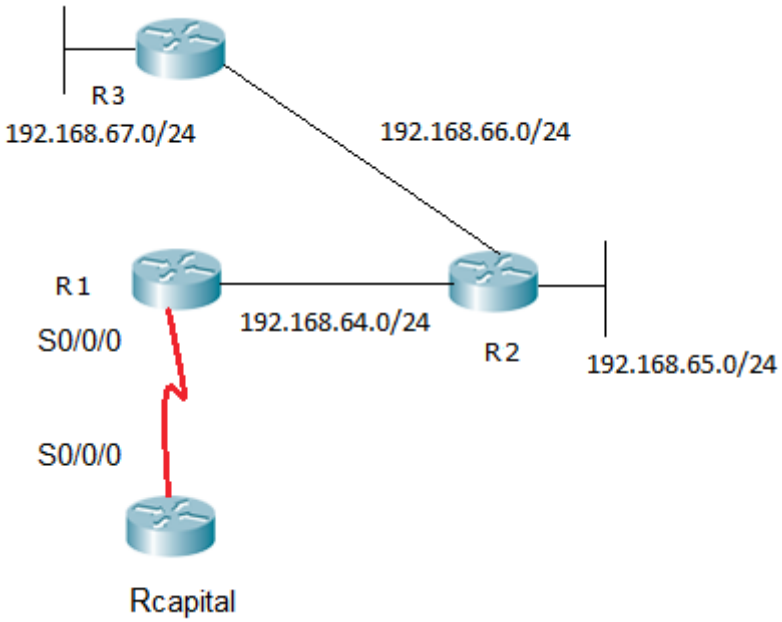


Figura 7.
Fuente: propia

Para resumir las rutas debemos tener presente los siguientes pasos:

- Escribir las redes que se van a resumir con su correspondiente valor en binario:
  - 192.168.64.0 - 11000000.10101000.01000000.00000000
  - 192.168.65.0 - 11000000.10101000.01000001.00000000
  - 192.168.66.0 - 11000000.10101000.01000010.00000000
  - 192.168.67.0 - 11000000.10101000.01000011.00000000
- Encontrar la máscara de subred, la cual se consigue contando de izquierda a derecha los ***bits*** hasta donde se encuentre una disparidad en los números; esto identifica que el resumen llega hasta este punto. La máscara que se obtuvo fue /22 la cual corresponde a 255.255.252.0.

  Este valor 255.255.252.0 es equivalente a la suma de cada uno de los octetos 1111 1111.11111111.111111**00**.00000000

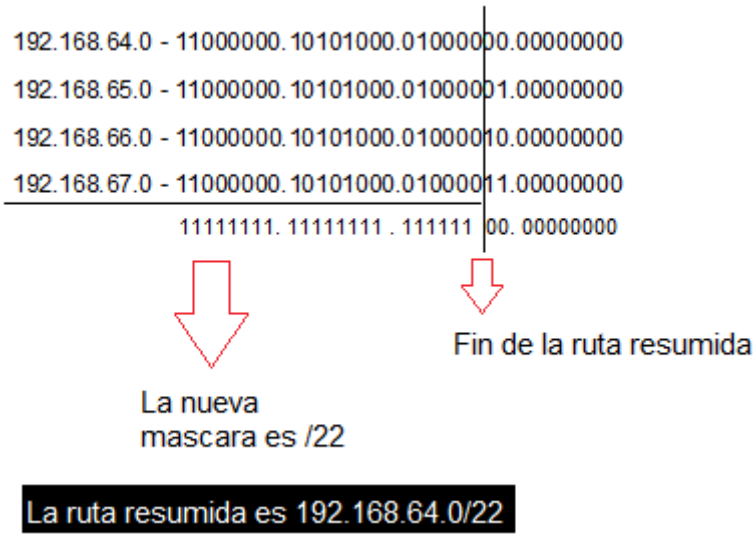


Figura 8.
Fuente: propia.

- La ruta resumida la ingresamos mediante el comando:

  Rcapital (config)# ip route 192.168.64.0 255.255.252.0 S0/0/0

- **Ruta estática flotante:** brinda la posibilidad a una organización de tener una ruta alternativa de respaldo garantizando la conectividad y el funcionamiento de la red. Se caracteriza por tener una distancia administrativa superior a la ruta estática predeterminada o estándar; esto depende de la configuración que establezca el administrador de la red.

  Ejemplo de este tipo de ruta es cuando el administrador de red está configurando su topología lógica mediante el protocolo RIPv2, el cual posee una distancia administrativa igual a 120. Lo ideal es configurar una ruta estática flotante con una distancia administrativa mayor que la que está manejando RIPv2. El proceso es el siguiente: en caso de una falla en la ruta suministrada por RIPv2, inmediatamente entra a modo de respaldo la ruta estática flotante.

Enrutamiento entre VLAN

En este apartado definiremos la importancia del enrutamiento entre VLAN y cómo se da el intercambio de información entre las VLAN, tema fundamental a la hora de diseñar e implementar redes informáticas. Para poder establecer el enrutamiento entre VLAN que se encuentran en segmentos de red diferentes es necesario implementar un *router* o un *switch* de capa 3.

VLAN
LAN virtuales que tienen la característica de agrupar elementos de manera lógica y física dentro de una red informática.

- ***Enrutamiento entre VLAN antiguo:*** el modo de funcionamiento de este tipo de enrutamiento parte de tener un router con conexiones por separado en cada una de las interfaces e implementar una configuración para subredes de manera individual. Estas conexiones de las interfaces estaban destinadas a los puertos del switch, dichos puertos se configuran en modo acceso.

  Para implementar este enrutamiento se deben seguir los siguientes pasos:

  - Las interfaces del ***router*** y del ***switch*** deben configurarse en modo troncal-***trunk***.

  - El proceso de enrutamiento entre VLAN lo desarrolla el ***router*** una vez admitido el tráfico de la VLAN en las interfaces que están en modo troncal que vienen del ***switch*** y realiza el enrutamiento entre las VLAN, a través de subinterfaces (interfaces virtuales múltiples vinculadas a una interfaz física).

    Para configurar una subinterfaz, entramos al router y definimos lo siguiente:

    - ***Router*** (config)# interface f0/0, se coloca un punto **(.)** y un número de subinterfaz, este suele asociarse al ID de la VLAN que se maneja en esa interfaz.

    Para que se reconozca la subinterfaz es vital configurar la encapsulación VLAN, seguida del número de la VLAN a que se encuentra asociada. Esta encapsulación se relaciona con el siguiente comando ***encapsulation dot1q 10***.

    Como es una subinterfaz debemos añadir la dirección IP seguida de la máscara de subred, la cual pertenece a la interfaz que está asociada. Después de esto se procede a habilitar la interfaz utilizando el comando ***no shutdown.***

    Para verificar el enrutamiento utilizamos el comando *show ip route*.

    Ejemplo:

    Router (config)# interface f0/0.10

    Router (config)# encapsulation dot1q 10

    Router (config)# ip address {***dirección-IP máscara-subred***}

    Router (config)# no shutdown

- ***Enrutamiento router-on-a-stick:*** presenta en su configuración una sola interfaz, la cual comunica al *router* con el *switch*. A diferencia del modo antiguo en el que se necesitaban varias interfaces, esta conexión física del *router* con el *switch* lleva un enlace troncal. En este modo de enrutamiento una sola interfaz realiza el enrutamiento a varias VLAN.

  Al igual que en el modo antiguo, se configura la interfaz en el *router* y el puerto asociado al *switch* de manera troncal. En el proceso de enrutamiento el mecanismo es el mismo que en el método antiguo, solo que esta vez todo el tráfico va dirigido por una sola interfaz.

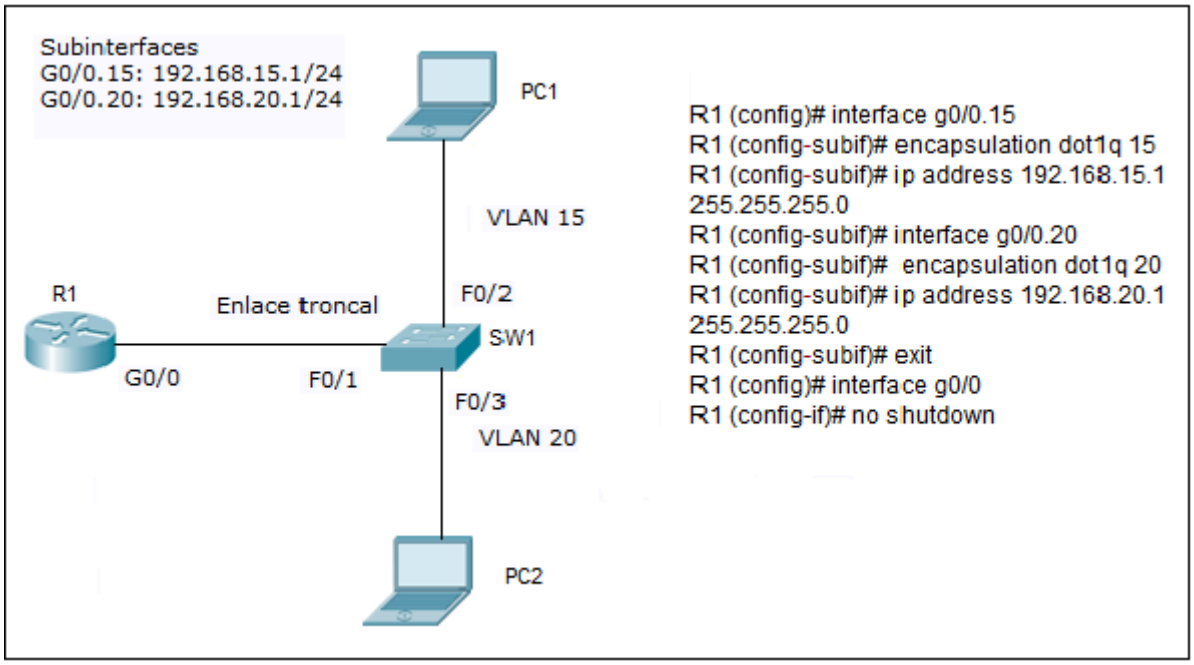


Figura 9. Configuración en el modo *router-on-a-stick*.
Fuente: propia

- ***Enrutamiento dinámico:*** este enrutamiento lo vemos en organizaciones medianas y grandes donde se necesita una actualización constante de las rutas. Se da mediante el encaminamiento de protocolos, los cuales actualizan automáticamente las rutas. Estos protocolos se basan en la tabla de enrutamiento para escoger la mejor ruta, brindan la posibilidad de establecer normas para que la red siempre esté actualizada. Ejemplo: una empresa en la que se permite escoger nuevas rutas en casos específicos donde la ruta presente inconvenientes y se procede a encontrar redes adyacentes.

Adyacentes
Se entiende como adyacente aquello que está próximo o cercano.

Los protocolos de enrutamiento dinámico se caracterizan por poseer:

- **Estructura de datos:** basa sus operaciones en la tabla de enrutamiento.

- **Mensajes:** se enfocan en relacionarse con los vecinos de manera que se pueda conocer qué cambios han sufrido dentro de la red.

- **Algoritmo:** desarrolla los protocolos con el objetivo de brindar información sobre los caminos y seleccionar la ruta adecuada.

Una de las desventajas de utilizar estos protocolos es el uso de recursos por parte del encaminador; además, la seguridad es baja, debido al envío constante de información por fuera de la red. La gran ventaja es que no se necesita de un administrador de manera permanente para realizar actualizaciones ante cambios dentro de la red informática.

Modo de operación de los protocolos dinámicos

1. Al encender el ***router***, este analiza su tabla de enrutamiento y se da lo que se conoce como actualización, donde se reconoce la manera en que están conectadas las rutas y por medio de qué interfaz se encuentran conectadas.

2. Una vez que se proceda a configurar los protocolos de enrutamiento, viene el proceso en que los ***routers*** asociados a la red interactúan entre ellos, lo cual manifiesta un constante envío de actualizaciones, garantizando identificar qué redes se encuentran vinculadas a cada enrutador. Esto lo hace mediante las interfaces que se encuentran activas.

3. Por último, el ***router,*** al recibir las actualizaciones, analiza si hay cambios dentro de la red y los registra en su tabla de enrutamiento. Esto lo hace periódicamente para garantizar la convergencia dentro de la red y seleccionar la mejor ruta. La convergencia se obtiene al momento de que todos los elementos dentro de la topología gocen de una información total de la red. La convergencia de protocolos como RIP se manifiesta de manera más lenta en comparación que los protocolos Eigrp y OSPF.

Convergencia

Se da cuando cada uno de los elementos o dispositivos conocen o tienen información de toda la red.

Tipos de protocolo de enrutamiento dinámico

Existen tres grupos de protocolos de enrutamiento dinámico:

- **Según el propósito:** los encontramos como protocolos de ***gateway*** interior (IGP) y protocolos de ***gateway*** exterior (EGP).

  Antes de entrar a analizar estos protocolos se debe conocer un término que va de la mano de estos: sistema autónomo (AS). Se denomina SA al grupo de redes administradas que poseen un encaminamiento dentro de una organización.

  - **IGP:** se caracterizan por tener la capacidad de relacionarse al interior de una organización en un sistema autónomo. Los protocolos de enrutamiento IGP más conocidos son RIP, Eigrp y OSPF.

  - **EGP:** se caracterizan por tener la capacidad de establecer relaciones entre sistemas autónomos; además, pueden coexistir en su funcionamiento varios protocolos IGP dentro de los EGP. Estos sistemas autónomos tienen una administración por separado, lo que beneficia el mantenimiento de la red. Los EGP utilizan unos ***routers*** conocidos como ***routers*** de borde, los cuales se encuentran al extremo de cada sistema autónomo. Los EGP utilizan el protocolo de enrutamiento dinámico BGP.

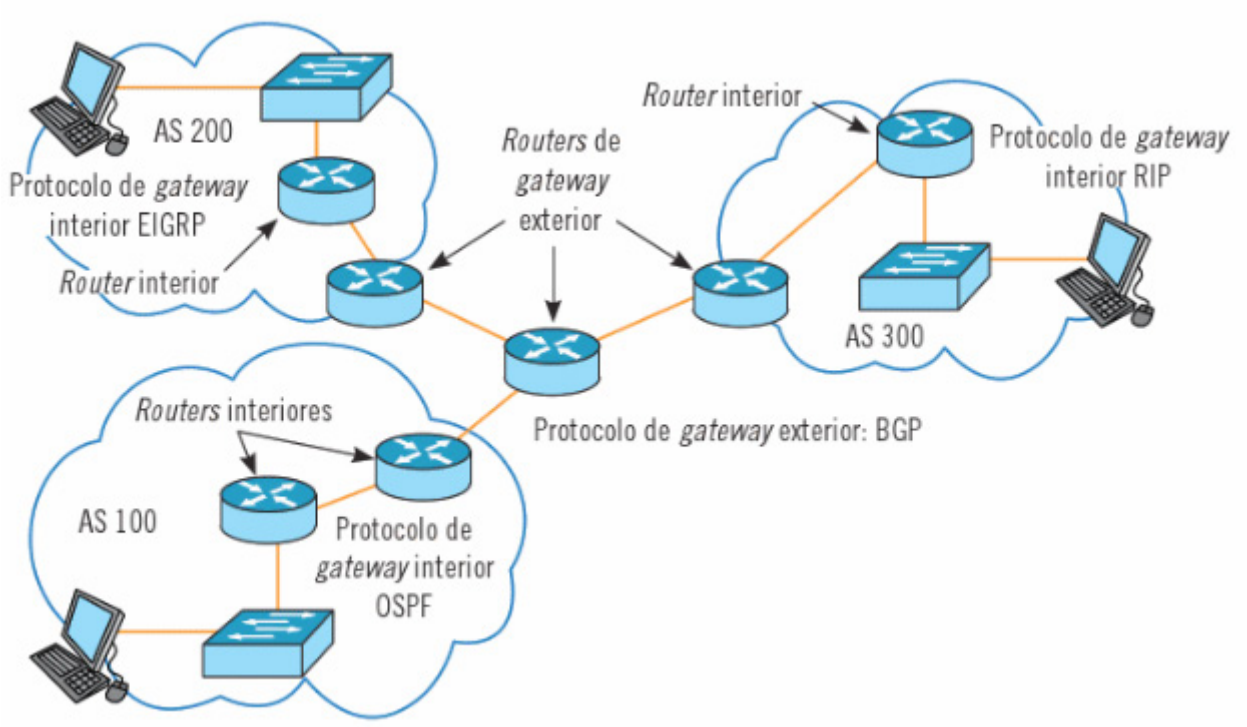


Figura 10. Protocolos de enrutamiento exterior e interior.
Fuente: Bellido Quintero (2014)

- **Según la operación:** los encontramos como vector distancia, protocolo de estado de enlace y protocolo vector de ruta.

- **Protocolo vector distancia:** se basa en dos parámetros implícitos en su nombre: la distancia, esta manifiesta el recorrido del origen al destino, y el vector, el cual identifica la dirección en que se encuentra ubicado el enrutador del siguiente salto o interfaz de salida hasta alcanzar el destino. El objetivo de los protocolos de vector distancia es identificar la ruta más corta determinando el sentido y la distancia en cualquier elemento de la red.

    - Los *routers* que implementan vector distancia tienen conocimiento parcial del camino para llegar a su destino. En su totalidad, el ***router*** tiene conocimiento sobre la métrica.

    - Los siguientes protocolos se identifican con IGP vector distancia IPv4: RIPv1, RIPv2, IGRP y Eigrp.

- **Protocolo de estado enlace**: se caracteriza por conocer toda la red. La manera en que se desempeñan los ***routers*** en este estado enlace les permite generar un mapa mediante el cual acceden a la mejor ruta para llegar al destino.

    - Este protocolo funciona en una red donde se provee de un diseño jerárquico. Se trabaja en función de la convergencia. Los protocolos de enrutamiento que se desempeñan mediante estado enlace son OSPF e IS-IS.

- **Protocolos de enrutamiento con clase y sin clase:** estos protocolos se caracterizan por el manejo de la información. No comparten información de la máscara de subred en el enrutamiento, mientras que los protocolos de enrutamiento sin clase sí lo hacen.

    - Los protocolos RIPv1 - Eigrp hacen parte de los protocolos con clase, debido a esto no manejan en su funcionamiento máscaras de subred de longitud variable, así como enrutamiento entre dominios sin clase (CIDR).

    - Los protocolos Eigrp, OSPF, BGP, etc., hacen parte de los protocolos sin clase. Se puede decir que en la actualidad se maneja en las empresas enrutamiento sin clase. Estos protocolos aceptan VLSM y CIDR. Los protocolos IPv6 forman parte de estos protocolos sin clase.

Protocolo RIP (*routing information protocol*)

Este protocolo, que nació en el año 1988, forma parte de la familia de los protocolos de vector distancia. Encontramos su especificación mediante la RFC 1058. Se caracteriza por:

- Su métrica corresponde al conteo de saltos. Esta equivale a 15. Después de este valor, se considera como paquete inaccesible.
- Anuncia sus ***updates*** cada 30 segundos.
- Distancia administrativa equivalente a 120.

Con el tiempo, RIP alcanza un nivel superior: evoluciona a RIPv2, el cual tiene las siguientes características:

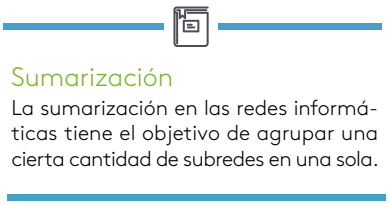
- Al ser un protocolo sin clase, admite VLSM y CIDR.
- Emplea la autenticación mediante la cual se garantiza actualizaciones de la tabla de enrutamiento.
- Reenvía actualizaciones a la dirección de multidifusión 224.0.0.9.
- Acepta rutas resumidas en las interfaces.

Configuración del RIP

- Con el comando *router rip* habilitamos el protocolo RIP.
- Con el comando *network* se designan las direcciones red que están directamente conectadas.
    - *Router (config)# router rip*
    - *Router (config-router)# network network-number*

Configuración RIPv2

Se siguen los mismos pasos de la configuración de RIP. Después, se añade el comando *version 2*. RIPv2 debe cambiar el proceso de sumarización automática, para esto utiliza el comando *no auto-summary*. Al deshabilitar la sumarización automática, el proceso de resumen de rutas ya no se manifiesta, con lo cual se concluye que se da la inclusión de cada una de las subredes asociadas con sus respectivas máscaras. Este comando *no auto-summary* se ingresa después del comando *version 2*.



Sumarización

La sumarización en las redes informáticas tiene el objetivo de agrupar una cierta cantidad de subredes en una sola.

- *Router (config)# router rip*
- *Router (config-router)# network network-number*
- *Router (config-router)# version 2*
- *Router (config-router)# no auto-summary*

Mediante el comando *passive-interface* se ahorran recursos del *router*, debido a que se suprimen las actualizaciones en las interfaces que no se estén implementando.

- *Router (config)# router rip*
- *Router (config-router)# passive-interface*
- *Router (config-router)# exit*

Verificación de la configuración RIP

El administrador de red en una organización debe garantizar una buena comprensión de los parámetros que se originan dentro de los siguientes comandos de verificación: *show ip route, show running-config y show ip protocols*.

El comando *show ip protocols* nos brinda información con respecto a los tipos de protocolos que se están implementando en el *router*. Mediante este comando se puede analizar toda la configuración de RIP, obteniendo lo siguiente:

- Versión de RIP está siendo usada.
- Interfaces que se encuentran activas, envío y recepción de actualizaciones.
- Comprobación de que el enrutador está dando información sobre las redes verdaderas.

Cuando se ingresa el comando *show ip route*, se obtiene información con respecto a las diferentes rutas que son obtenidas mediante el protocolo RIP y que encontramos en la tabla de enrutamiento. RIP se identifica en la tabla de con la letra R.

Protocolo IGRP (interior gateway routing protocol)

Es un protocolo de Cisco que forma parte de la familia de los protocolos de vector distancia. Publica sus ***updates*** cada 90 segundos y se puede implementar en redes grandes donde se adapta a los cambios dentro de la red. Esto se conoce como escalabilidad. Este protocolo utiliza dos métricas el BW y retardo. Hoy en día IGRP no se utiliza, en cambio se utiliza una versión mejorada Eigrp, este protocolo no será estudiado en esta asignatura.

Protocolo IS-IS (*intermediate system to intermediate system*)

Encontramos su especificación ISO 10589; este aporta soporte IP y se especifica en la RFC 1195. Forma parte de la familia de los protocolos de estado enlace junto con el protocolo OSPF. Como es un protocolo sin clase acepta VLSM y sumarización manual. El proceso de sincronización en los caminos de manera total se da en rango de 10 minutos.

IS-IS implementa unos paquetes Hello cada 10 segundos para comunicarse con los ***routers*** vecinos. Cada paquete Hello lleva consigo toda la información que adquirió con respecto a los ***routers*** vecinos. Al momento de que un ***router*** se manifiesta con una respuesta la cual trae consigo una igualdad se procede a tener una relación con el vecino. Esta relación se establece con la intención de llevar a cabo la comunicación. Con una comunicación efectiva se produce una adyacencia. Al tener la adyacencia, todos los ***routers*** vecinos intercambian información de carácter estado enlace. Posterior a este proceso, el objetivo esperado es lograr la convergencia, la cual se alcanza cuando cada uno de los enrutadores tiene conocimiento de toda la red.

Protocolo Eigrp (*open source patf firts*)

Es un protocolo IGP que evolucionó de IGRP. Forma parte de la familia de los protocolos de vector distancia. Acepta VLSM y sumarización de rutas. Eigrp tiene un proceso más rápido en las actualizaciones, lo cual conlleva a que la convergencia incremente su velocidad.

Eigrp implementa paquetes Hello no tan complejos que le permiten a los ***routers*** establecer adyacencias con los ***routers*** vecinos. Al conocer sus ***routers*** vecinos, implementa un protocolo de transporte seguro el cual verifica una entrega segura.

Protocolo OSPF (*open shortest path first*)

Este protocolo tiene sus orígenes a finales de los años 80, RFC 1131. Ya en el año 1991 aparece la versión 2, OSPFv2, RFC 1247; esta sufre una evolución en el año 1998: RFC 2328. Forma parte de la familia de los protocolos de estado enlace; también acepta VLSM, o sea, es un protocolo de enrutamiento sin clase. OSPF implementa áreas para su desarrollo, esto lo hace un protocolo eficaz. En esta asignatura se analizará OSPF con área única.

Características OSPF

- La distancia administrativa equivale a 110.
- Tiene la capacidad de operar con redes de tamaño pequeño y grandes redes, facilitando la escalabilidad.
- Los tiempos para la convergencia son reducidos.
- Los ***routers*** implementan un algoritmo que se conoce como SPF (***shortest path first***) de Dijkstra, al momento de escoger la mejor ruta. SPF se caracteriza por agrupar los diferentes costos que se encuentran en las rutas para alcanzar el destino. Una vez establecidas las rutas, OSPF se encarga de guardarlas en la de enrutamiento para su posterior uso.

BIBLIOGRAFÍA

Aznar López, A. (2005). *La red internet. El modelo TCP/IP*. Madrid, España: Grupo Abantos Formación y Consultoría.

Bellido Quintero, E. (2014). *Equipos de interconexión y servicios de red (UF1879)*. Málaga, España: IC Editorial.

Boronat Seguí, F. (2013). *Direccionamiento e interconexión de redes basadas en TCP/IP: IPv4/IPv6, DHCP, NAT, encaminamiento RIP y OSPF*. Valencia, España: Editorial de la Universidad Politécnica de Valencia.

Carceller Cheza, R. (2013). *Servicios en red*. Madrid, España: Macmillan Iberia S. A.

Castaño Ribes, R. J. (2013). *Redes locales*. Madrid, España: Macmillan Iberia S. A.

Hallberg, B. (2007). *Fundamentos de redes*. Madrid, España: McGraw-Hill Interamericana.

Hillar, G. C. (2004). *Redes: diseño, actualización y reparación*. Buenos Aires, Argentina: Editorial Hispano Americana S. A.

Íñigo Griera, J. (2008). *Estructura de redes de computadores*. Barcelona, España: Editorial UOC.

Jiménez Camacho, R. (2014). *Análisis del mercado de productos de comunicaciones (UF1869)*. Málaga, España: IC Editorial.

Martínez Yelmo, I. (2015). *IPv6-Lab: entorno de laboratorio para la adquisición de competencias relacionadas con IPv6*. Madrid, España: Universidad de Alcalá.

Molina Robles, F. J. (2014). *Servicios de red e Internet*. Madrid, España: RA-MA Editorial.

Moreno Pérez, J. C. (2014). *Sistemas informáticos y redes locales*. Madrid, España: RA-MA.

Santos González, M. (2014). *Diseño de redes telemáticas*. Madrid, España: RA-MA Editorial.

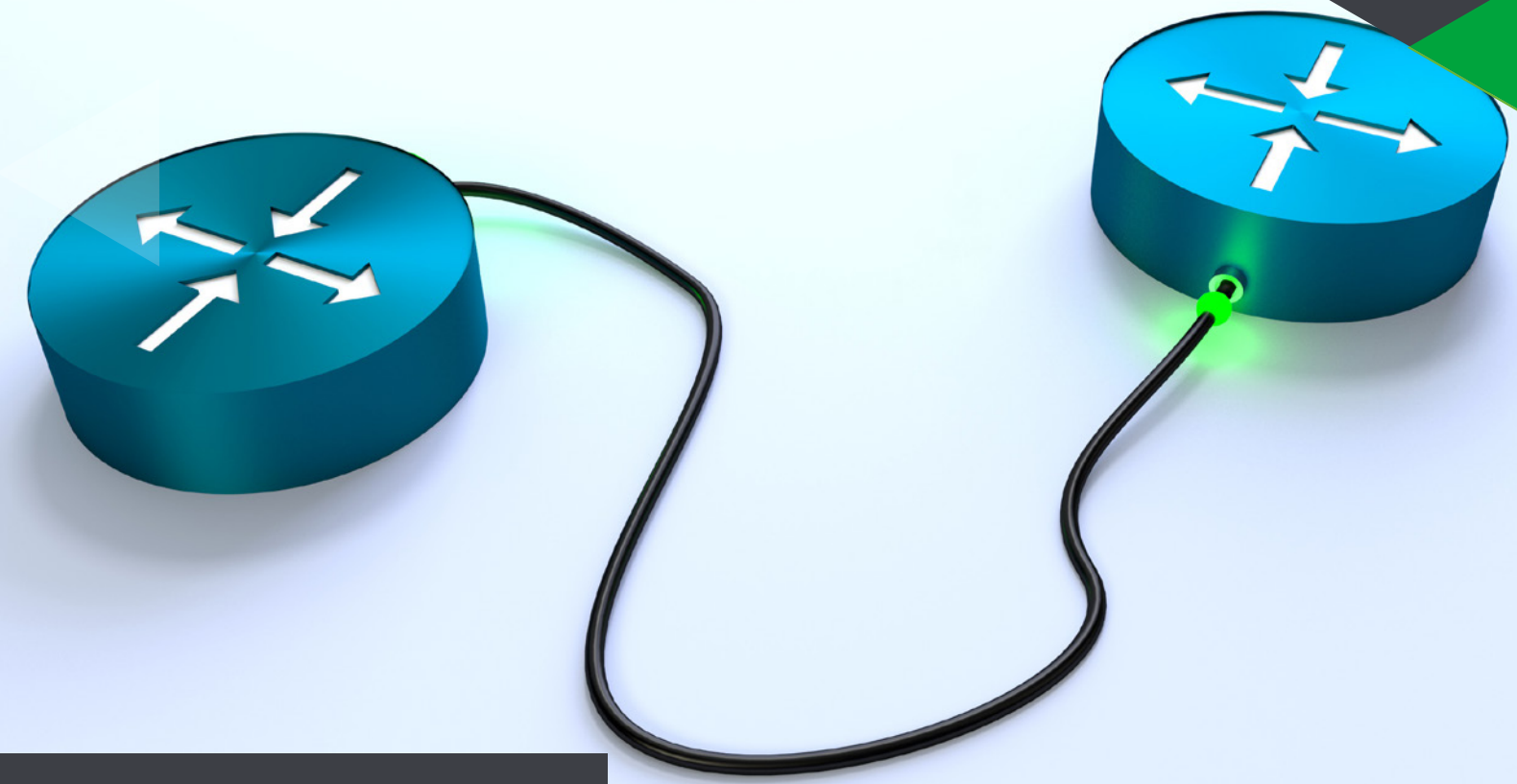
Velte, T. J. (2008). *Manual de Cisco®*. Madrid, España: McGraw-Hill Interamericana.

ENRUTAMIENTO Y CONFIGURACIÓN DE REDES

Ricardo López Bulla

EJE 3

Pongamos en práctica



Fuente: Shutterstock/202776187

AREANDINA
Fundación Universitaria del Área Andina
MIEMBRO DE LA RED ILUMNO

INTRODUCCIÓN

Las destrezas que se adquieren al desarrollar prácticas de laboratorio mediante softwares de simulación como Packet Tracer generan en el estudiante competencias que van a ser implementadas y plasmadas en su vida laboral dentro de las organizaciones, lo cual es una razón válida para poner a prueba conocimientos adquiridos en el transcurso de esta asignatura a través de estas prácticas.

Al momento de conocer las necesidades que van surgiendo en las empresas, el futuro administrador de la red estará en la capacidad de afrontar nuevos retos y brindar una solución idónea ante los acontecimientos que se presenten. Saber interpretar cada uno de los comandos que se presentan, ya sea mediante la tabla de enrutamiento o los comando show, permitirá una excelente administración de dicha red. En este eje, exploraremos el protocolo de enrutamiento dinámico OSPF hasta su versión actualizada OSPFv3.

Protocolo de enrutamiento dinámico OSPF

Introducción al OSPF

En el eje 2 abordaremos temas básicos sobre el OSPF. En este eje nos enfocaremos en la importancia que tiene este protocolo para las redes informáticas que se implementan en las organizaciones. Se dará una doctrina práctica y real sobre cómo configurar este protocolo e interpretar cada uno de sus comandos.

El OSPF es un protocolo de estado enlace que tiene su origen en necesidades de las redes informáticas que otros protocolos como el RIP no podían suplir; en específico, acepta CIDR, converge de manera rápida, publica sus actualizaciones mediante estado enlace a sus routers vecinos y desarrolla su modo de operación a través de áreas que dividen las redes informáticas en unidades más pequeñas dentro de la red para optimizar y administrar los procesos. El área 0 es la principal.

Backbone

Área principal de la red a la cual se conectan las demás áreas dentro de una organización, permitiendo la interacción de estas.

En la siguiente figura podemos apreciar el área *backbone* o área 0, la cual se trabajará en esta asignatura.

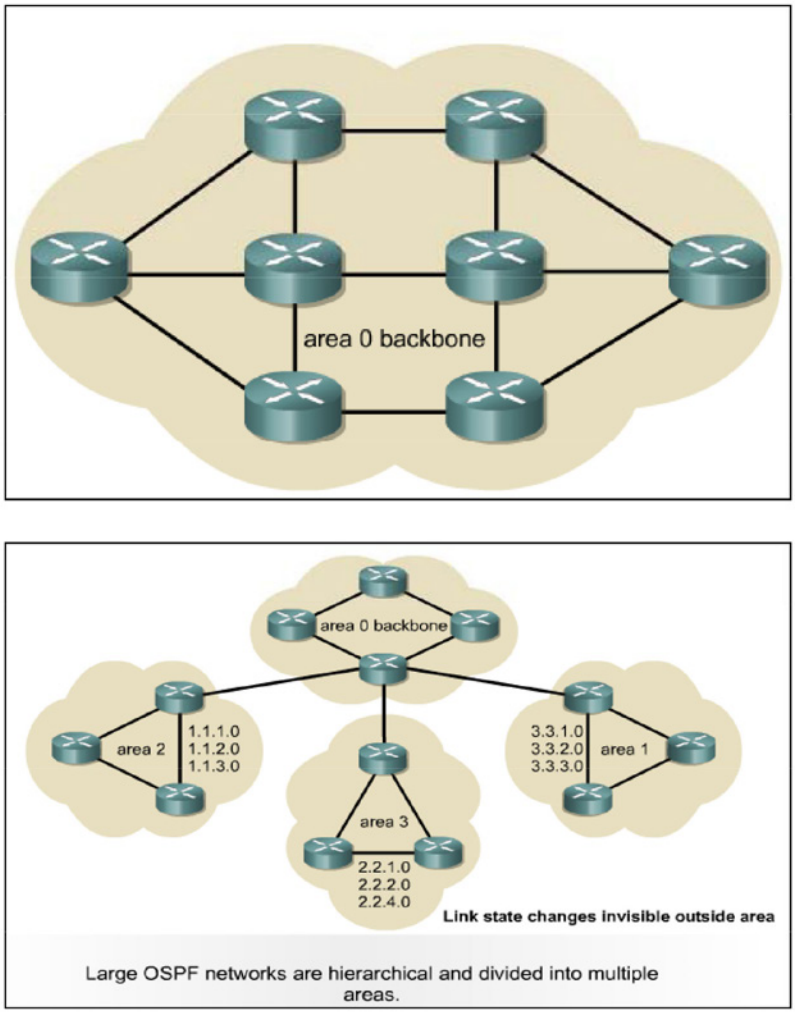


Figura 1. Área *backbone* o 0
Fuente: http://informatica.uv.es/iiguia/AER/Tema3_Routing.pdf

Encapsulamiento OSPF

En la siguiente figura se puede apreciar que la encapsulación OSPF se manifiesta sobre IP, mediante el campo "mensaje OSPF con un valor 89". Este va estar ubicado en la cabecera del datagrama. Además, los mensajes van a tener un tráfico a través de una dirección IP *multicast*.

Datagrama
Cadena de información a nivel de capa 3-red, transmitida por un medio.

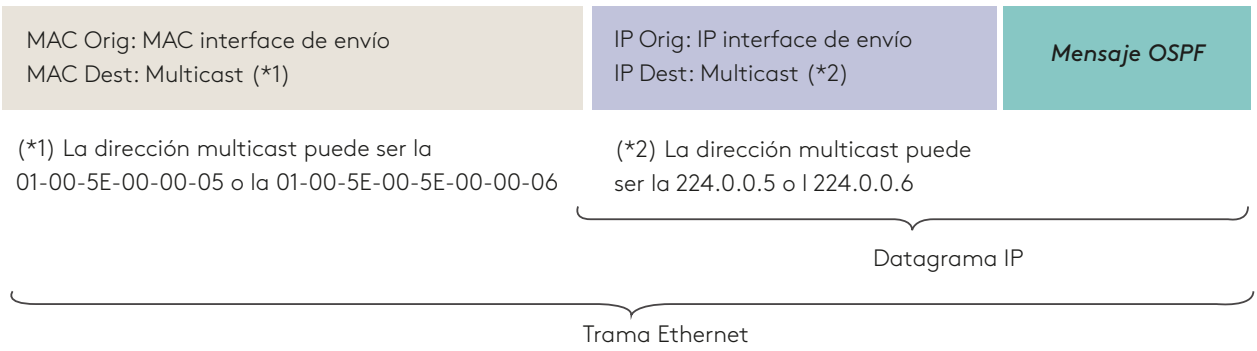


Figura 2.
Fuente: Boronat Seguí (2013)

Wildcard

Es una clase de máscara que facilita seleccionar direcciones IP. Si comparamos la *wildcard* con una máscara de subred tradicional, encontramos que esta define el tamaño de la red, mientras que la *wildcard* brinda la posibilidad de elegir el tráfico que se desea procesar. La máscara *wildcard* tiene una representación específica en bits:

- 0: representa la existencia de una coincidencia.
- 1: representa la no existencia de una coincidencia (se ignoran).

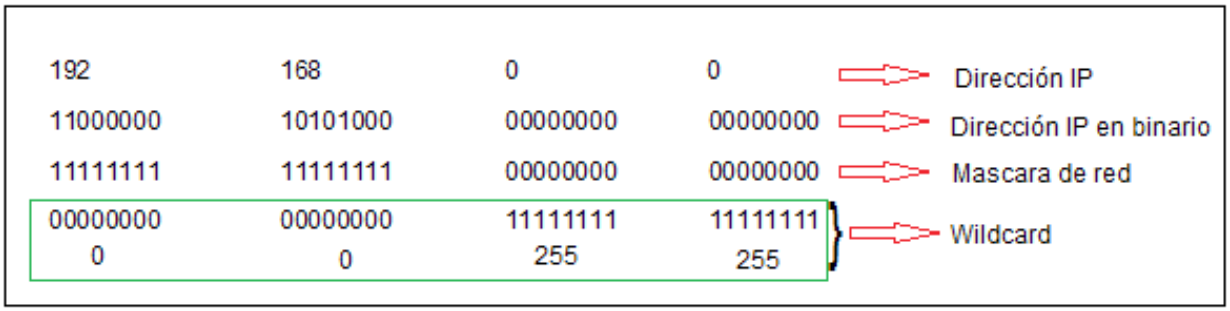


Figura 3.
Fuente: propia

Costo: OSPF

La métrica que está asociada a OSPF es el costo**,** el cual se define como un incremento para el envío de paquetes a través de las interfaces. Esta métrica se basa en la suma de cada uno de los valores que se encuentran en las interfaces. Dicho costo posee una relación inversa con el ancho de banda, la manera de obtener el ancho de banda es la siguiente:

Costo= 10^8/ancho de banda de la interfaz – bps

Por ejemplo, para interfaz *fastethernet* el costo por defecto es 1.

Costo= 10^8/100Mbps= 1

Para configurar el costo manualmente, se ingresa en la interfaz el siguiente comando:

Router(config-if)# ip ospf cost[valor]

Video

Para afianzar los conocimientos, los invito a ver la videocápsula *Direccionamiento e interconexión de redes basada en TCP/IP: IPv4/IPv6, DHCP, NAT, Encaminamiento RIP y OSPF* en la página principal del eje.

Bps
(Bits por segundo): unidad que representa el ancho de banda.

Existen cinco tipos de paquetes en OSPF:

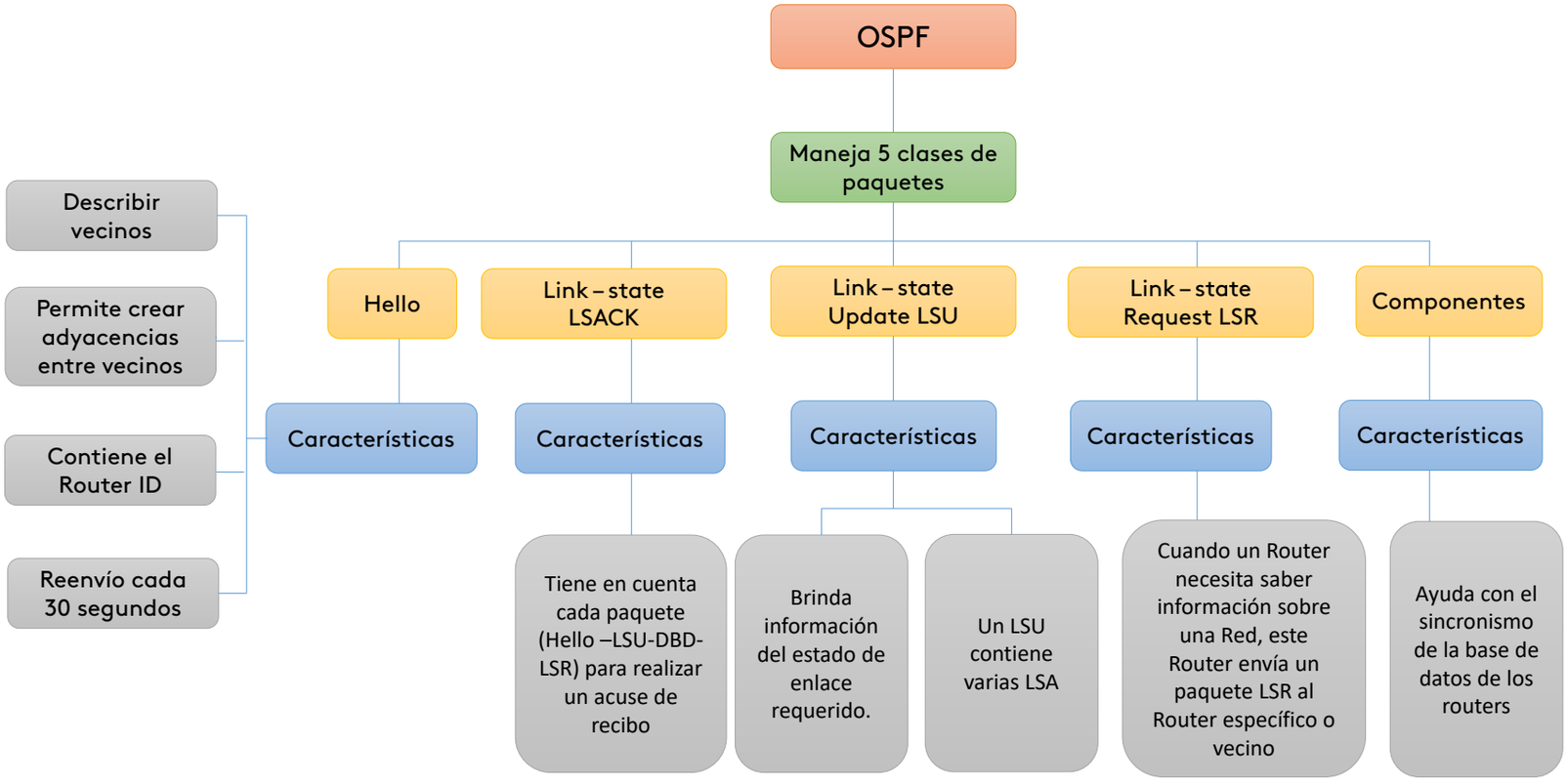


Figura 4. Paquetes de OSPF
Fuente: propia

En los paquetes Hello de OSPF se envían actualizaciones a las direcciones *multicast* 224.0.0.5 o 224.0.0.6 cada 30 segundos en redes con acceso múltiple sin *broadcast* NBMA (*non-broadcast multi-access*) y cada 10 segundos para redes múltiples de acceso con *broadcast*. Ejemplo: Ethernet.

NBMA

Redes que no presentan en su configuración difusión broadcast.

Los paquetes LSA (anuncios del estado del link) informan acerca del costo y el estado del enlace a todos los routers que forman parte de una red informática, lo cual conlleva a una respuesta o a un acuse de recibo al router emisor. Esto es contraproducente debido al consumo de recursos como ancho de banda y tráfico en la red. Es por esto que se realiza un proceso de escogencia de un DR (router designado) y un DBR (router designado de reserva) dentro de la red.

Router designado y *router* designado de reserva

Al presentarse varios *routers* con actualizaciones de enlace es necesario tener un *router* en el cual se centralicen dichas actualizaciones. Estamos hablando del DR, el cual tendrá a cargo funciones como la transmisión y el sincronismo dentro de la red. El BDR entrará a funcionar al momento de presentarse una falla en el DR. Para destacar, los *routers* OSPF tienen un parámetro que se llama prioridad por defecto con valor de 1. Este parámetro se puede manipular para determinar cuál va a ser el DR y el BDR. Se prioriza que el *router* con el mayor valor de prioridad asignado será el DR; por consiguiente, el *router* con el segundo valor más alto vendrá a ser el BDR. El valor al que se puede configurar la prioridad está entre 0 y 255. El comando que permite establecer la prioridad en el *router* DR es el siguiente:

- *Router*(config)# interface fastethernet 0
- *Router*(config-if)# ip ospf priority *número*

Configuración básica de OSPF

El comando *router ospf* habilita el protocolo OSPF:

R1(config)# router ospf [id del proceso]

El ID registra el proceso que está llevando a cabo el *router*. Este ID del proceso es un número en el rango 1-65535.

R1(config)# router ospf 1

Una vez habilitado el OSPF procedemos a publicar las redes que están directamente conectadas. Este proceso se realiza de la siguiente manera: *network* + dirección de red + máscara *wildcard* + *area (ID del área)*.

R1(config)# router ospf 1

R1(config-config)# network [network address – wildcard] área 0

Verificación de OSPF

Existen varios comandos que nos brindan la información adecuada sobre el correcto funcionamiento del protocolo OSPF:

- *R1# show ip route:* visualiza la tabla de enrutamiento donde se aprecian las rutas aprendidas.
- *R1# show ip ospf interface:* visualiza las interfaces en las diferentes áreas; también nos brinda información sobre las adyacencias.
- *R1# show ip ospf database:* visualiza el ID del *router* y del proceso.
  - *R1# show ip ospf neighbor detail*: visualiza cada uno de los vecinos asociados al *router* incluyendo el estado en que se encuentran.
  - *R1# show ip protocols:* visualiza parámetros como la métrica, red y temporizadores.

Adyacencias
Se originan en el momento de intercambio de información entre dos routers.

OSPFv2

Versión definida en el año 1991: RFC 1247 OSPFv2 (forma parte de la familia de los protocolos de estado enlace - *Link State*), mejorada en el año 1998: RFC 2328. La versión 3 (para IPv6) de OSPF se define un poco más tarde en el año 1999: RFC 5340, y se mejora en el año 2008: RFC 5340.

Configuración OSPFv2

Analicemos la manera de configurar OSPFv2 mediante la siguiente topología (en cada uno de los pantallazos visualizamos cada paso).

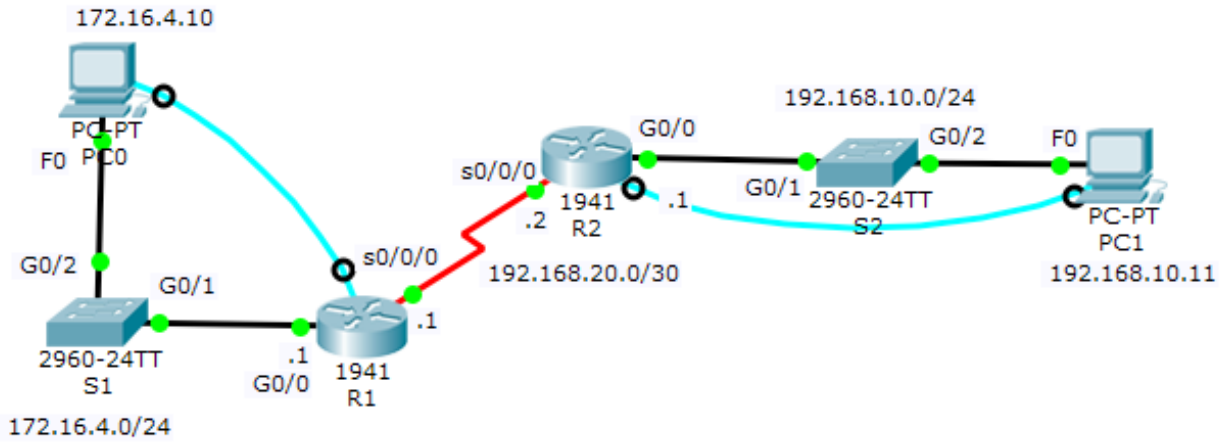


Figura 5.
Fuente: propia

- Partimos de la premisa de que se han configurado las interfaces de los *routers*.

- Habilitamos OSPFv2 en R1, mediante el comando *router ospf [id-proceso]*. Este valor ID-proceso está en un rango 1-65535.

- Procedemos a configurar los ID de los *routers*. Este ID lo encontramos de manera predeterminada en los *routers* o puede ser manipulado por el administrador de red. Es importante tener un ID habilitado en el *router*, ya que brinda la posibilidad de diferenciar o conocer los *routers* dentro de un dominio OSPF, así como los mensajes originados de estos. Además, mediante los ID, los *routers* forman parte de la elección del DR. Este proceso se origina al inicio del establecimiento de OSPF. El elemento con la prioridad mayor se elige como DR. En caso de que no exista prioridad configurada, se procede a la elección del DR con el mayor ID.

  Para configurar el ID en los *routers* se utiliza el siguiente comando: *router-id [id-router]*. En este comando debemos incluir un número en formato dirección IPv4 (en R1 se asignará para esta práctica el ID 1.1.1.1 y para R2 el ID 2.2.2.2). En la figura 7, podemos identificar este comando resaltado en color rojo, así como la verificación del mismo mediante el comando *show ip protocols*.

- Se procede a publicar las redes que están directamente conectadas a los *routers* mediante las interfaces. Este proceso se lleva a cabo con el comando: network {dirección-red} máscara-wildcard area {id-área}.

En la figura 7 podemos evidenciar el parámetro *network* resaltado de color azul. En este punto, es necesario calcular la *wildcard*. Por ejemplo: para obtener la *wildcard* de la red conectada al R1: 172.16.4.0/24, restamos a la máscara de subred el valor de 255.255.255.255. En este caso, la máscara de subred es:/24= 255.255.255.0

```
  255.255.255.255
 -255.255.255.0
-----------------
  0 . 0 . 0 . 255
```

Al realizar la resta, se obtiene la *wildcard:*

Figura 6.
Fuente: propia

Interfaz pasiva

En la actualidad es importante tener efectividad, seguridad y optimización en los recursos asociados a las redes informáticas dentro de las organizaciones. Por esta razón, protocolos como el OSPF están enfocado a lograr este objetivo. Una de las maneras es implementar parámetros como interfaces pasivas. Como se sabe, OSPF inunda con mensajes todas las interfaces dentro de la red que cuenten con OSPF en estado enlace por defecto; así, al administrador de red solo debe interesarle que los mensajes sean enviados por las interfaces que va a interconectar con otros routers con OSPF habilitado. Para configurar las

interfaces pasivas se utiliza el siguiente parámetro: passive-interface dentro de la configuración del protocolo OSPF. Este parámetro ayuda a que el tráfico no se manifieste por las interfaces que el administrador considere no apropiadas. Este proceso se realiza de la siguiente manera:

- *R1(config)# router ospf 10*
- *R1(config-router)# passive-interface fastethernet 0*
- *R1(config-router)# end*

En la figura 7 podemos evidenciar el parámetro de interfaces pasivas resaltado de color verde.

Finalizada la configuración en el R2, se empiezan a enviar los mensajes Hello de adyacencia con R1. Esto lo apreciamos en la figura 7 con el parámetro resaltado de color naranja.

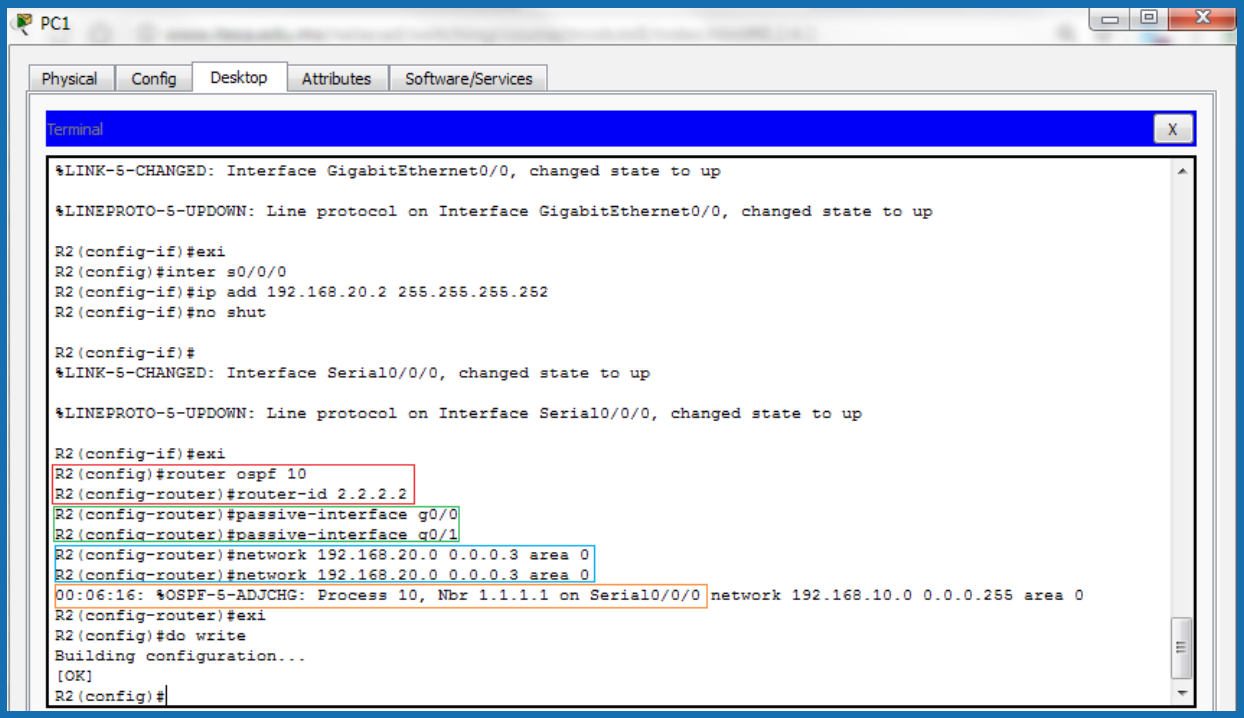


Figura 7.
Fuente: propia

Verificación del protocolo OSPF

La figura que encontraremos a continuación se compone de dos partes: la primera parte (figura 8-I) muestra cómo comprobar mediante un PING desde la PC0 a la PC1 sí existe convergencia. Como resultado de este PING, se puede observar que sí hay convergencia en la topología. En la segunda parte (figura 8-II) se visualiza si el protocolo está bien configurado a través de los comandos *show ip protocols* (se resaltan todos los parámetros en color naranja) y *show ip route*. En la tabla de enrutamiento se puede identificar que el protocolo OSPF está operando, ya que aparece reflejado con el carácter "O".

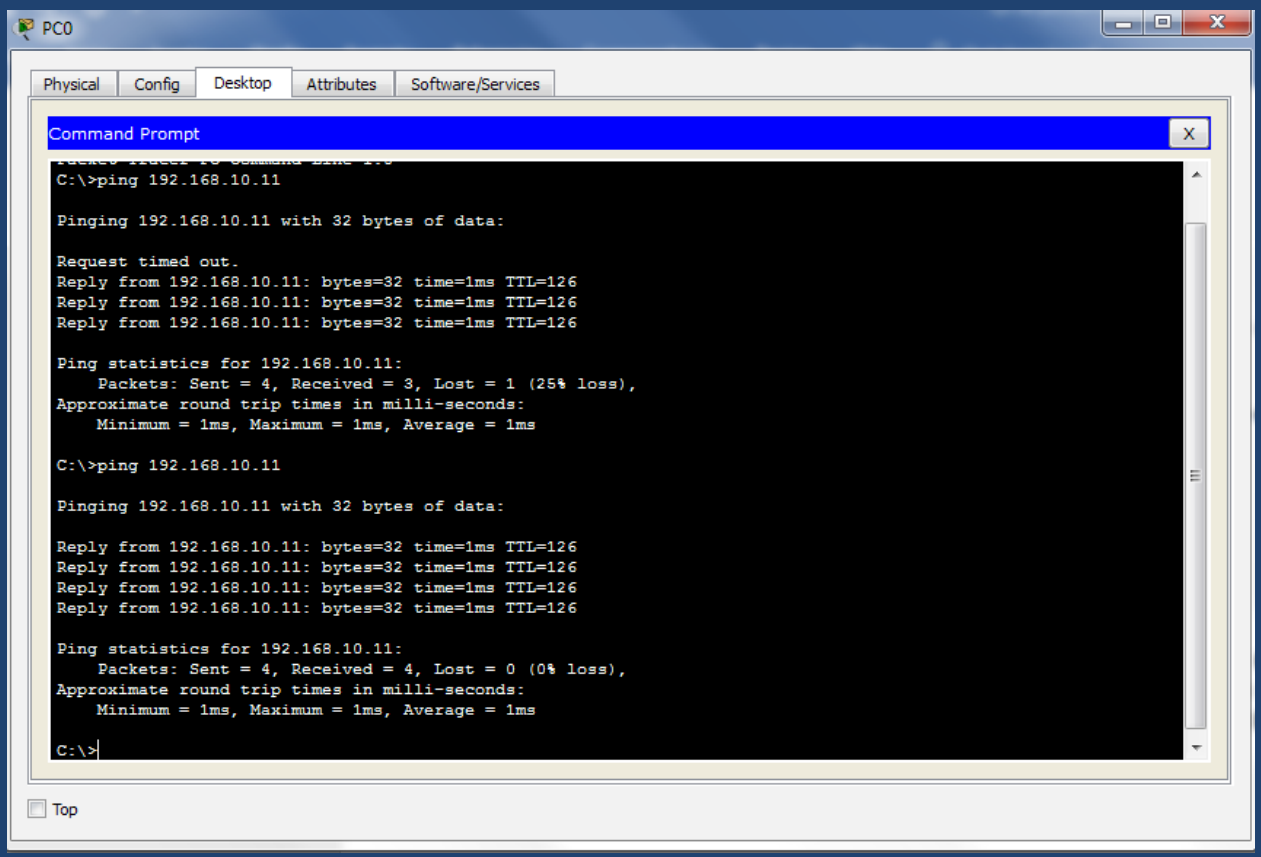


Figura 8-I.
Fuente: propia

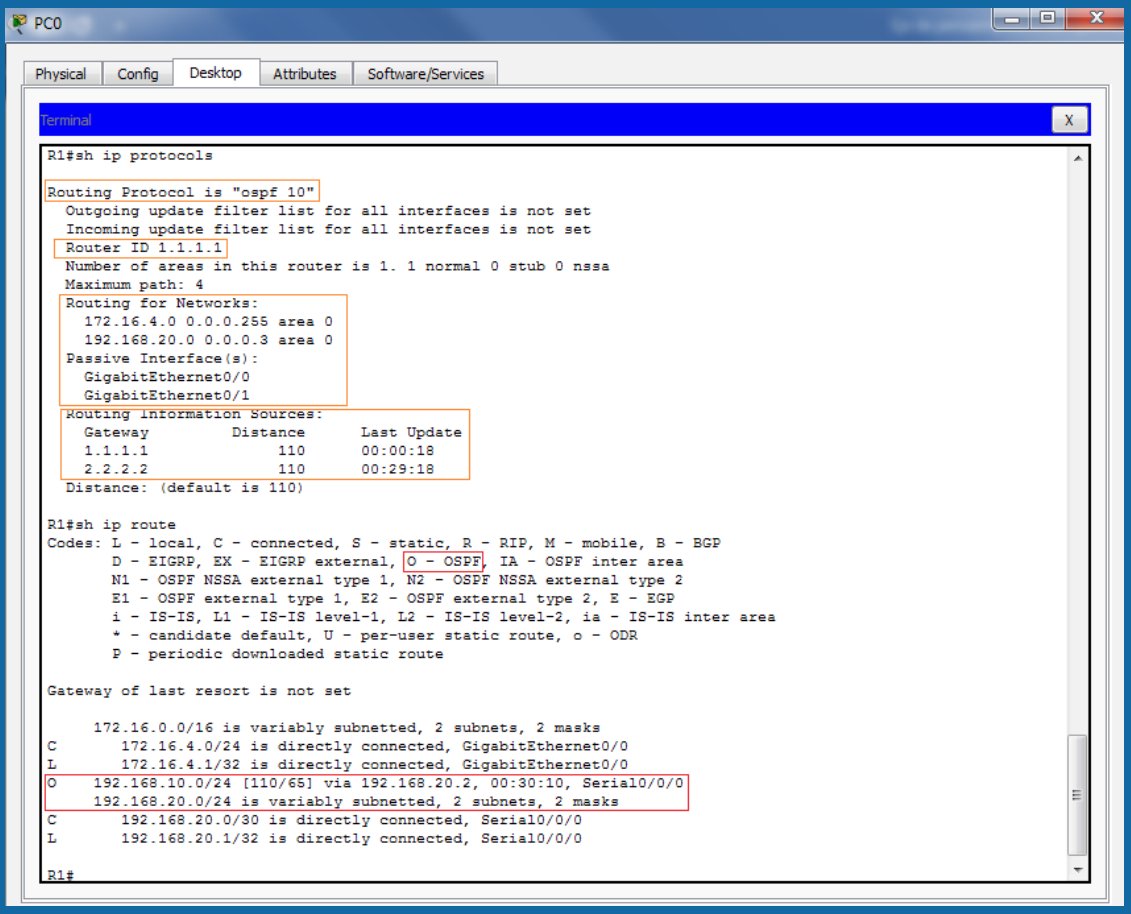


Figura 8-II.
Fuente: propia

OSPFv3

OSPFv3 tiene su origen en la aparición del protocolo IPv6, RFC 2740. Esta es la gran diferencia respecto a las demás versiones de OSPF.

Características

- Para establecer la configuración de OSPF dentro del *router* se debe partir del siguiente parámetro: en el modo de configuración global *ipv6 unicast-routing*.

- Al igual que OSPFv2, OSPFv3 utiliza el parámetro SPF, con el objetivo de identificar las rutas adecuadas. Además de esta semejanza, tiene otras como: la métrica (costo), se maneja el concepto de áreas dentro de las redes, los tipos de paquetes

OSPF son Hello, DBD, LSR, LSAck y LSU, se manejan las adyacencias entre *routers* vecinos y funciona igual para la elección del DR y BDR.

- La dirección en OSPF correspondiente a multidifusión es FF02::6.
- OSPFv3 da a conocer sus redes con el comando de interfaz: *"ipv6 ospf id-proceso area id-área"*.
- Las direcciones IPv6 apropiadas para que un enrutador logre comunicarse desde su origen hasta el destino sin ir más lejos o que pueda relacionarse con otros elementos son las direcciones *link-local* (enlace-local).

Configuración OSPFv3

En la siguiente topología encontraremos la convergencia de las dos versiones de OSPF versión 2 y 3 (IPv4 e IPv6). La tecnología Dual-Stack permite que interactúen en una misma topología de red ambos protocolos. Además de la topología, encontraremos los diferentes comandos para configurarla.

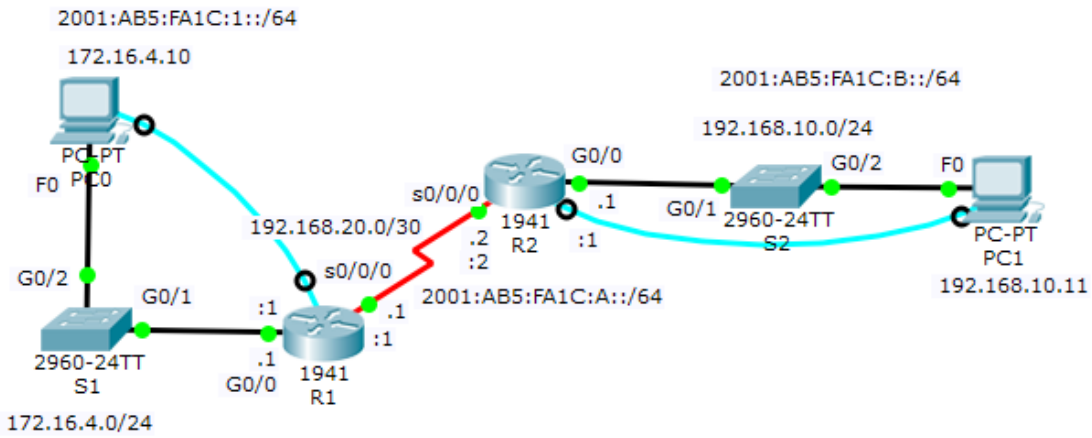


Figura 9. Topología práctica en Packet Tracer, OSPF versión 2 y 3
Fuente: propia

Para la configuración del protocolo OSPFv3 debemos habilitar el enrutamiento a través de IPv6 en los *routers*, después asignar las direcciones de unidifusión global en el enrutador:

- *R1(config)# ipv6 unicast-routing*
- *R1(config)# interface g0/0*

Unidifusión

Se comprende como el envío de información de uno a uno, en términos de dispositivos dentro de una red informática.

- *R1(config-if)# ipv6 add {network-address}*
- *R1(config-if)# no shutdown*
- *R1(config-if)# exit*

Una vez configuradas las direcciones de unidifusión global se procede a configurar las direcciones *link-local* en cada una de las interfaces de los dispositivos:

- *R1(config)# interface g0/0*
- *R1(config-if)# ipv6 address FE80::1 link-local*
- *R1(config-if)# exit*

Después de configurar las direcciones de unidifusión y *link-local* se configuran los ID de los enrutadores. Para este proceso habilitamos OSPF mediante el comando *ipv6 router ospf {id-proceso}*. El ID-proceso se encuentra en un valor dado en el rango de 1 a 65535 igual que en OSPFv2; este valor es designado por el administrador de la red en el modo de configuración global de los enrutadores. A continuación, encontraremos la configuración del ID-proceso con un valor igual a 10 en el R1, de la topología encontrada en la figura 9:

- *R1(config)# ipv6 router ospf 10*
- *R1(config-rtr)# router-id 1.1.1.1*
- *R1(config-rtr)# exit*

Al tener configurados los ID en los enrutadores se habilita OSPFv3 en las interfaces del *router*. Para esto no es necesario utilizar el comando *network* implementado en OSPFv2. En OSPFv3 se designa el ID específicamente sobre las interfaces, lo cual se realiza con el comando *ipv6 ospf {id-proceso} area {id-área}* dentro de la interfaz. El valor del área es 0 (área *backbone*):

- *R1(config)# interface g0/0*
- *R1(config-if)# ipv6 ospf 10 area 0*
- *R1(config-if)# exit*
- *Comandos de verificación OSPFv3*

Los comandos de verificación en OSPFv3 son:

- ***R1# show ipv6 protocols:*** brinda información acerca del protocolo implementado, el ID y las interfaces asignadas con este protocolo.
- ***R1# show ipv6 ospf interface brief:*** brinda información acerca de las interfaces que tienen habilitado OSPFv3.
- ***R1# show ipv6 ospf neighbor:*** brinda información de los vecinos, verificando adyacencia entre estos.
- ***R1# show ipv6 route ospf:*** brinda información de las rutas establecidas en la tabla de enrutamiento.

BIBLIOGRAFÍA

Aznar López, A. (2005). *La red internet. El modelo TCP/IP*. Madrid, España: Grupo Abantos Formación y Consultoría.

Bellido Quintero, E. (2014). *Equipos de interconexión y servicios de red (UF1879)*. Málaga, España: IC Editorial.

Boronat Seguí, F. (2013). *Direccionamiento e interconexión de redes basadas en TCP/IP: IPv4/IPv6, DHCP, NAT, encaminamiento RIP y OSPF*. Valencia, España: Editorial de la Universidad Politécnica de Valencia.

Carceller Cheza, R. (2013). *Servicios en red*. Madrid, España: Macmillan Iberia S. A.

Castaño Ribes, R. J. (2013). *Redes locales*. Madrid, España: Macmillan Iberia S. A.

Hallberg, B. (2007). *Fundamentos de redes*. Madrid, España: McGraw-Hill Interamericana.

Hillar, G. C. (2004). *Redes: diseño, actualización y reparación*. Buenos Aires, Argentina: Editorial Hispano Americana S. A.

Íñigo Griera, J. (2008). *Estructura de redes de computadores*. Barcelona, España: Editorial UOC.

Jiménez Camacho, R. (2014). *Análisis del mercado de productos de comunicaciones (UF1869)*. Málaga, España: IC Editorial.

Martínez Yelmo, I. (2015). *IPv6-Lab: entorno de laboratorio para la adquisición de competencias relacionadas con IPv6*. Madrid, España: Universidad de Alcalá.

Molina Robles, F. J. (2014). *Servicios de red e Internet*. Madrid, España: RA-MA Editorial.

Moreno Pérez, J. C. (2014). *Sistemas informáticos y redes locales*. Madrid, España: RA-MA.

Santos González, M. (2014). *Diseño de redes telemáticas*. Madrid, España: RA-MA Editorial.

Velte, T.J. (2008). *Manual de Cisco®*. Madrid, España: McGraw-Hill Interamericana.

ENRUTAMIENTO Y CONFIGURACIÓN DE REDES

Ricardo López Bulla

EJE 4

Propongamos

Fuente: Shutterstock/258980774

AREANDINA
Fundación Universitaria del Área Andina
MIEMBRO DE LA RED ILUMNO

INTRODUCCIÓN

Cada día, el ser humano se ve en la necesidad de desarrollar habilidades y de **cualificarse** para estar a la vanguardia en lo concerniente al área donde se desempeña, así como para estar en capacidad de coordinar, dirigir y tomar decisiones con responsabilidad en las organizaciones, sobre todo los administradores de redes informáticas, quienes tienen a su disposición herramientas fundamentales para que una organización funcione de la mejor manera. Ejemplos de estas decisiones son las políticas internas que se manejan en la red informática y la manera en que se accede a la información, ya sea de forma estática o dinámica.

Cualificar

Cualificar es dar a alguien formación especializada para que desempeñe una actividad profesional.

Dentro de estas políticas es fundamental establecer parámetros para garantizar la seguridad de la información dentro de las empresas. En este eje, el administrador de la red obtendrá la capacidad de gestionar políticas de seguridad mediante las listas de control de acceso (ACL).

Listas de control de acceso

Para lograr un funcionamiento eficaz de la red informática, los administradores deben identificar qué tipo de tráfico puede fluir dentro la red y qué tipo se debe restringir. Con los enrutadores, el administrador puede lograr un filtrado básico de la información que facilita la *World Wide Web* (www), que es la red mundial de ordenadores. Esto es posible gracias a las listas de control de acceso (ACL).

Funcionamiento

Como su nombre lo expresa, las ACL son listas que brindan una instrucción precisa de los paquetes que se van a permitir o denegar dentro de las interfaces del enrutador. Estos parámetros tienen unas premisas para operar: fuente y destino del mensaje, tipo de tráfico o protocolo y número de puerto asociado TCP/UDP.

Una vez creada una ACL, se puede vigilar y administrar el tipo de tráfico que circula por las redes. Esto lo implementa el ***router*** mediante los diferentes protocolos, como IP e IPX (intercambio de paquetes entre las redes).

UDP
TCP (transmission control protocol): protocolo de la capa 4 (transporte) del modelo OSI. TCP descrito RFC 793. Protocolo orientado a la conexión: negocia y establece una conexión (o sesión) permanente entre los dispositivos de origen y de destino antes de reenviar tráfico.

Empleabilidad de las ACL

- Permiten realizar una selección en el tráfico que se maneja en las redes informáticas, garantizando un mejor rendimiento de la red.
- Brindan un nivel básico de seguridad a las redes informáticas dentro de las empresas. Esta seguridad se manifiesta en el acceso que se brinda en la red.
- Permiten administrar la clase de información, con el fin de limitar la cantidad de paquetes que se propaga en las redes.

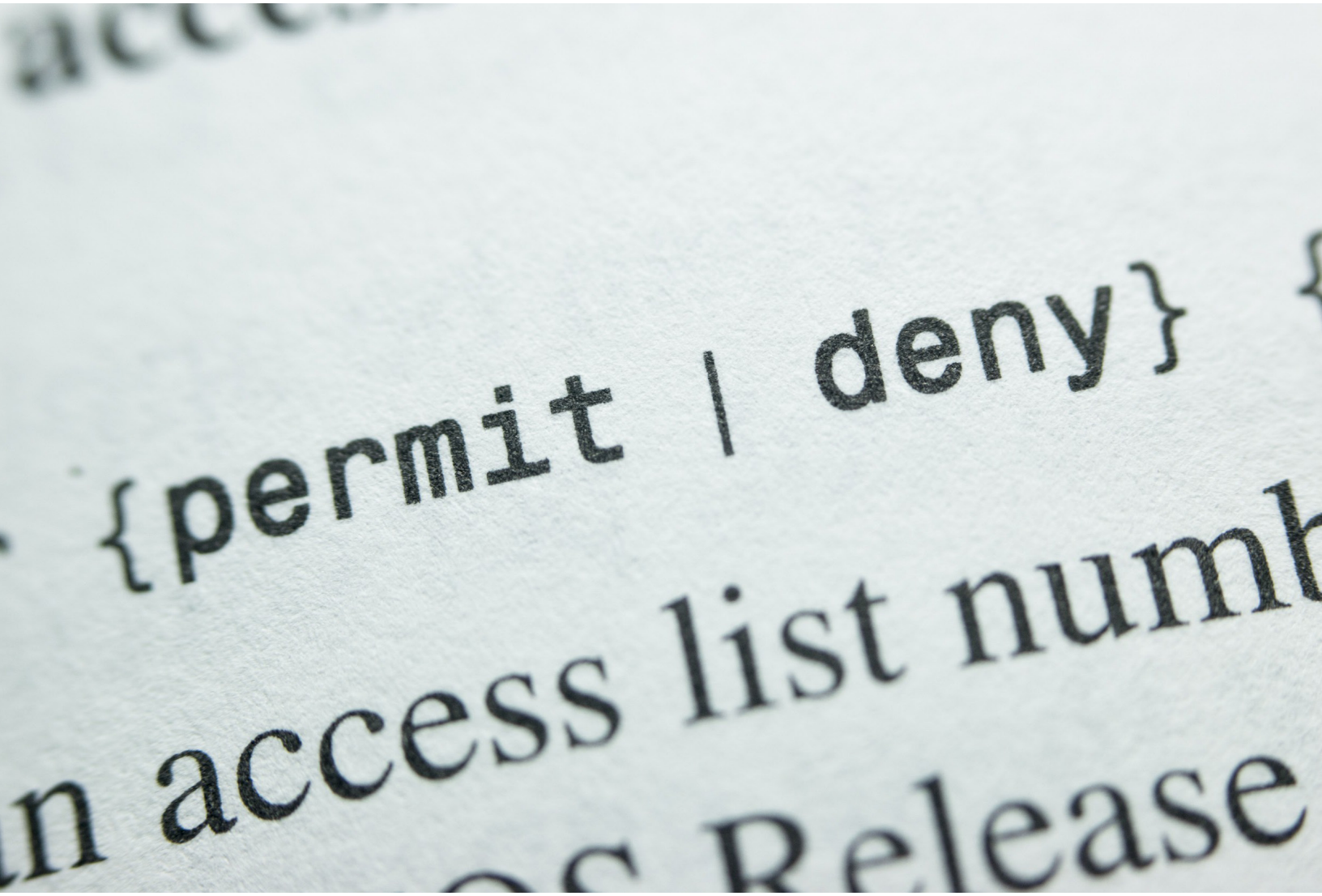


Figura 1. Sentencias ACL
Fuente: shutterstock/353579582

¿Cómo funcionan las ACL?

Las ACL son listas de sentencias de instrucciones: *permit* (permitir) y *deny* (denegar). Estas se definen como entradas de control de acceso (ACE) que concretan los paquetes que pueden entrar y reenviarse mediante las interfaces de los enrutadores. A medida que los paquetes se encaminan a las interfaces de los ***routers***, estos analizan el paquete y miran si se puede enrutar. Una vez analizado este parámetro, los enrutadores detallan si existe una ACL en el paquete. Si hay una respuesta positiva, el paquete es contrastado en la lista de enrutamiento del ***router***. Si este paquete es aceptado, inmediatamente es analizado en la tabla de enrutamiento en donde se establece la interfaz de destino. Luego, los enrutadores analizan si la interfaz de destino posee una ACL. Si no es así, el paquete se reenvía a la interfaz de destino.

Las ACL se configuran de dos maneras, según el tráfico que maneje el diseñador dentro de la red:

- **ACL de entrada:** se caracterizan porque los paquetes que llegan al ***router*** tienen un proceso antes de alcanzar la interfaz de salida del enrutador. Esto ahorra recursos a la red. Si el paquete no coincide en la tabla de enrutamiento, se descarta.

- **ACL de salida:** se caracterizan porque los paquetes que llegan se encaminan a la interfaz de salida, lo cual precisa un análisis a través de la ACL de salida. Se suelen implementar cuando se presenta un único filtro a los paquetes que tienen su origen en múltiples interfaces de entrada, antes de alcanzar la misma interfaz de salida.

Encaminar
Dirigir algo hacia un punto determinado.

Por defecto
Automáticamente. Si no, se elige otra opción.

Tipos de ACL IPv4

Existen dos tipos de ACL IPv4: estándar y extendida. En esta asignatura abordaremos las ACL estándar, las cuales se pueden crear asignando un *nombre* o un *número* para caracterizarlas. Ejemplo: las ACL estándar tienen un rango numérico de 1 a 99 y 1300 a 1999.

Las ACL estándar se caracterizan porque brindan la posibilidad de permitir o denegar el tráfico de las direcciones IPv4 de origen. La manera en que se configura una ACL estándar es la siguiente:

R1(config)# access-list {numero – lista acceso} {deny/permit} {dirección-red} wildcard

A continuación, encontraremos ejemplos de ACE y su interpretación:

a. *R1(config)# access-list 10 deny 192.168.1.1*: no hay máscara *wildcard*. Cuando sucede esto, se asimila que la máscara está por defecto 0.0.0.0. Esta ACE deniega la dirección 192.168.1.1.

b. *R1(config)# access-list 10 permit 192.168.1.0 0.0.0.255:* permite el ***host*** 192.168.1.0 o cualquier *host* dentro de la subred 192.168.1.0.

c. *R1(config)# access-list 10 deny 192.168.1.1 0.0.255.255:* deniega cualquier ***host*** perteneciente a la red 192.168.0.0.

d. *R1(config)# access-list 10 permit 192.168.1.1 0.255.255.255:* permite cualquier ***host*** perteneciente a la red 192.0.0.0.

Un parámetro fundamental dentro de las ACL estándar es habilitar las ACE dentro de las interfaces del enrutador. Para configurar este parámetro partiremos del ejemplo "b". El comando habilita la sentencia como filtro de salida sobre la interfaz. Esta configuración se implementa en la siguiente gráfica.

Filtro
Sistema de selección en un proceso, según criterios previamente establecidos.

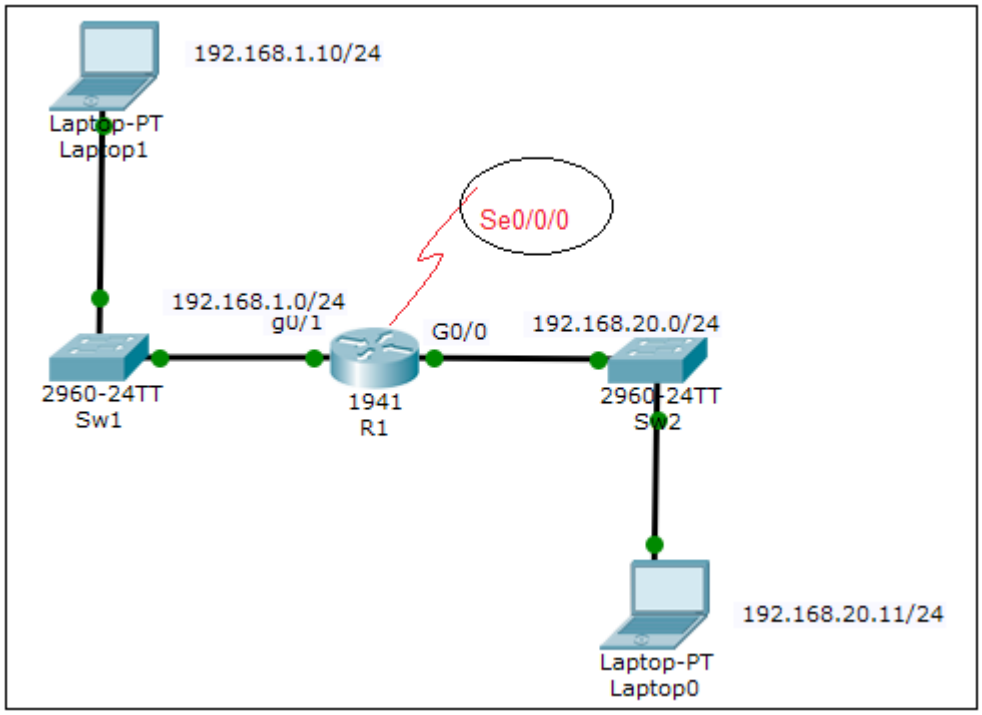


Figura 2.
Fuente: propia

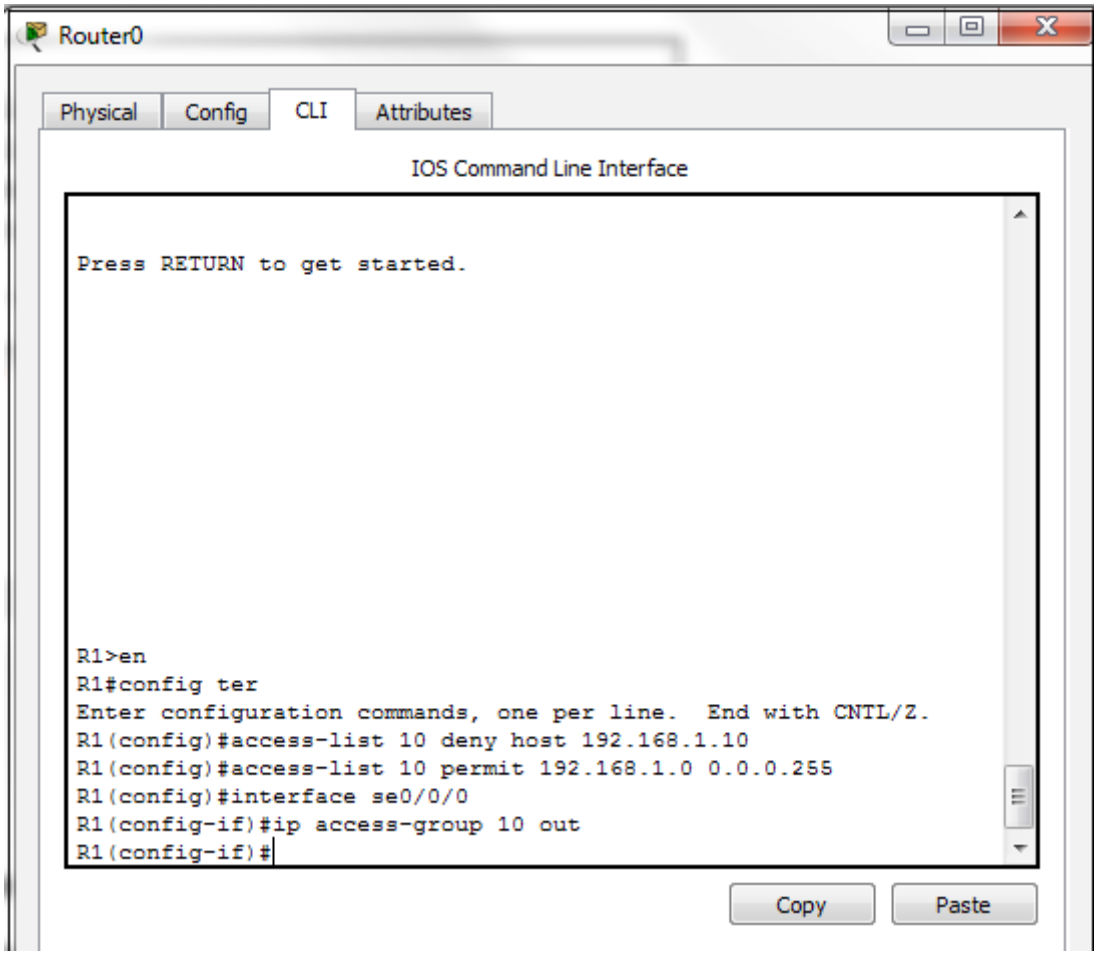


Figura 3.
Fuente: propia

Verificación de las ACL

Mediante el comando *show access-lists* se puede comprobar si las ACL están bien configuradas. En la siguiente figura se aprecian las sentencias ACE.

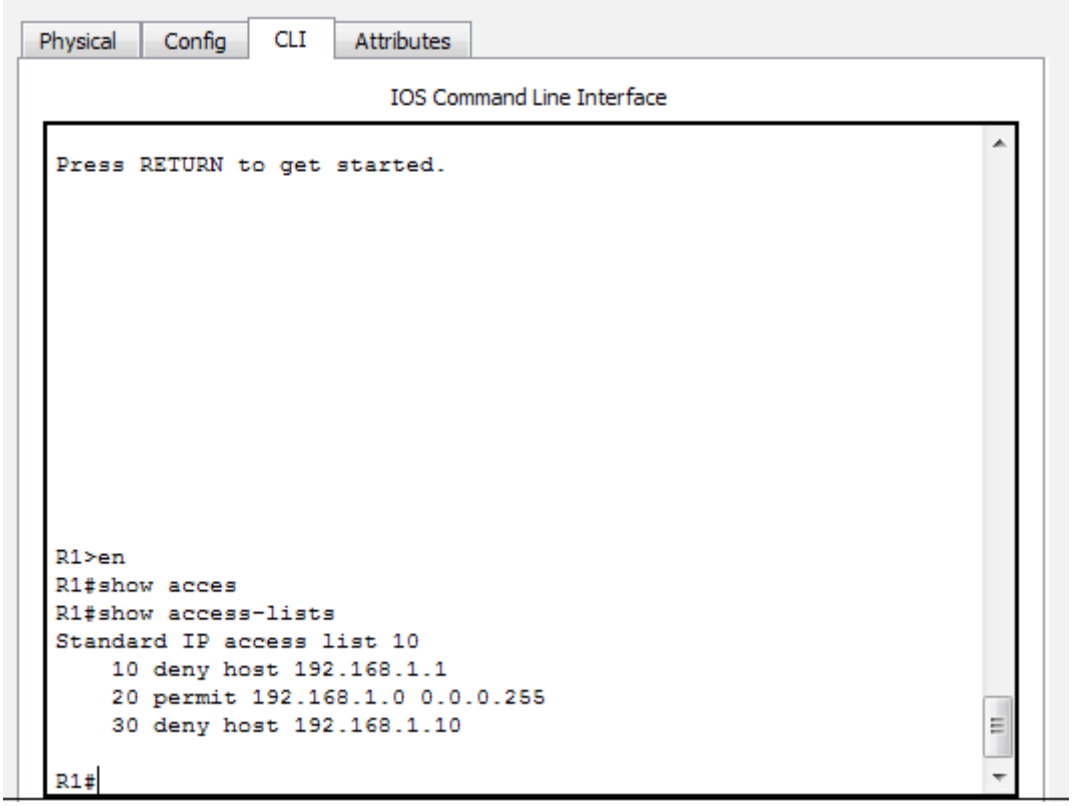


Figura 4.
Fuente: propia

La configuración que se planteó forma parte de las ACL estándar con número. A continuación, se darán a conocer las ACL estándar con nombre, las cuales tienen una particularidad: facilitar su funcionamiento y entendimiento. Al configurar estas ACL los comandos varían. A continuación, se muestra el proceso de configuración.

En el modo configuración global del ***router*** configuramos:

R1(config)# ***ip access-list {standard} name***

Los nombres se caracterizan porque conllevan números y letras. Se asimila la manera en que se escriben, con mayúscula o minúscula. Deben ser únicos y nunca deben comenzar por un número.

Una vez creada la ACL con nombre se procede a crear las sentencias: denegar o permitir el tráfico. Esto se realiza en el modo de configuración de la ACL con nombre de la siguiente manera:

R1(config)# ***ip access-list {standard} name***

R1(config-std-nacl)# ***{permit / deny / remark} network-address {wildcard}***

> **¡Importante!**
>
> El comando remark adiciona un comentario en las entradas de las ACL para entenderlas mejor a la hora de implementarlas.

Por último, se configuran las ACL con nombre a una interfaz. Es importante detallar si los paquetes llegan (*in*) o salen de la interfaz (*out*). Se recomienda escribir los nombres en mayúscula, esto permite reconocer las sentencias. A continuación, se muestra cómo se configura este comando:

R1(config)# ***interface g0/0***

R1*(config-if)# ip Access-group name [in / out]*

- **ACL extendidas:** estas se identifican porque brindan la posibilidad de filtrar el tráfico mediante caracteres como: protocolo que se implementa, dirección IPv4 de origen/destino y puertos TCP o UDP de origen/destino.

- **ACL-IPv6:** son sentencias parecidas a las manejadas con el protocolo IPv4. En IPv6 encontramos un solo tipo de ACL, el cual corresponde a la ACL extendida con nombre en IPv4.

TCP
TCP (transmision control proctocol: protocolo de control de transmisión). Protocolo orientado a conexión, fiable.

UDP
UDP (user datagram protocol: protocolo de datagramas de usuario). Protocolo no orientado a conexión, no fiable, pero más rápido.

Configuración

Como se mencionó, el objeto de estudio de esta asignatura abarcará solo las ACL estándar. Las ACL extendidas son implementadas a través del protocolo IPv6, por este motivo solo mencionaremos los comandos. Esto no será evaluado.

Figura 5. Protocolo de internet versión 6
Fuente: shutterstock/486567814

En el modo de configuración del enrutador se coloca el comando: *ipv6 access-list name*. Después se deniega o permite el tráfico con el objetivo de especificar los paquetes que se descartarán y cuáles se dejarán pasar o reenviar. Esto se implementa con el comando: *{deny / permit} ipv6 network-address ipv6*. Con estos comandos se crea la ACL IPv6.

Network address translation (NAT)

Surge de la necesidad de preservar las direcciones IPv4 públicas (se describe en el RFC 1631). Este objetivo lo alcanza NAT al momento en que las organizaciones adquieren una dirección IPv4 privada y están en la capacidad de traducir las direcciones IP privadas a IP públicas cuando lo consideren necesario. NAT brinda seguridad y privacidad a las organizaciones, debido a que no permite que las direcciones IPv4 sean visibles a las redes del entorno.

Al momento de establecer NAT sobre los enrutadores se pueden tener no solo una dirección IPv4, sino muchas IP (públicas). Este grupo de direcciones se conoce como: conjunto de NAT. Estos enrutadores que operan con NAT se conocen como fronterizos o de borde en una red informática. Se caracterizan por poseer un solo medio para conectarse con la red adyacente. Una vez que el dispositivo al interior de la red informática quiera establecer contacto con un dispositivo en otro dominio de red, lo hace mediante los enrutadores fronterizos con NAT habilitado.

Términos asociados a NAT

Existen términos indispensables para comprender el funcionamiento de NAT. La red al interior se compone del conjunto de redes que están dispuestas a ser traducidas (red interna). La red externa la componen las redes remotas o adyacentes.

Adyacente
Situado en la inmediación o proximidad de algo.

NAT se compone de varios tipos de direcciones: dirección local interna, dirección global interna, dirección local externa y dirección global externa. A continuación, encontraremos una descripción de las direcciones:

- **Dirección interna:** se traduce por medio de NAT en los dispositivos.
- **Dirección externa:** asociada al dispositivo receptor.
- **Dirección local:** segmentos de red a nivel interno de la red.
- **Dirección global:** asociada en el segmento externo de la red.

Al combinar los términos "interna-externa'' con "global-local" se pueden determinar direcciones puntuales en las redes informáticas. Por ejemplo, al tener dirección local interna se hace referencia a la dirección IP de origen analizada al interior de la red. Al presentarse la dirección global interna se hace referencia a la dirección IP analizada desde la red remota o adyacente. La dirección local externa hace referencia a la dirección de destino, analizada desde la red remota o adyacente. La dirección global interna hace referencia a la dirección de destino analizada desde la red interna.

NAT realiza sus funciones de dos maneras:

- **Estática:** se distingue porque en su configuración asigna direcciones IP mediante las direcciones globales y locales.
- **Dinámica:** se distingue porque en su configuración se coloca una dirección IP no registrada a otra dirección IP que sí lo está del grupo de direcciones IP que posee un registro.

Configuración

- **NAT estática:** en el modo de configuración global del ***router*** se implementan los siguientes comandos:

R1(config)# ip nat inside source static ip-local ip-global. Con esta configuración se establece una conversión de manera estática entre una dirección IP local interna y una dirección IP global interna.

R1(config)# interface g0/0 **(se designa la interfaz interna)**

R1(config-if)# ip nat inside

Después se designa la interfaz externa del enrutador mediante el comando:

R1(config)# interface g0/1

R1(config)# ip nat outside

- **NAT dinámica (de carácter temporal):** en el modo de configuración global del ***router*** se implementan los siguientes comandos:

  - *R1(config)# ip nat pool name ip-inicial ip-final {mascara-red / longitud-prefijo}:* se define el grupo de direcciones que se va a implementar.

  - *R1(config)# access-list lista_acceso permit wildcard:* se implementa una ACL para tener presente a cuáles ***hosts*** se les va a permitir o denegar el tráfico.

  - *R1(config)# ip nat inside source list lista de acceso pool nombre:* permite establecer la NAT dinámica partiendo de la dirección IP de origen.

  - *R1(config-if)# ip nat inside:* permite establecer la interfaz interna.

  - *R1(config-if)# ip nat outside:* permite establecer la interfaz externa.

Verificación NAT

Para verificar que la configuración de NAT está de la mejor manera se utilizan los siguientes comandos:

- *R1# show ip nat translations:* determina las conversiones activas.
- *R1# show ip nat statistics:* determina las estadísticas de conversión.

Ventajas

- Seguridad a la red.
- Se preservan las direcciones al momento de traducirlas y administrarlas de manera interna por parte de las organizaciones.
- Ahorro en los recursos de la red como, por ejemplo, el tiempo que gastaban las redes en redirigir cada ***host*** y que necesitaban acceder a redes adyacentes.

Figura 6. Servidor DHCP
Fuente: shutterstock/716347543

Protocolo DHCP

Este protocolo de configuración dinámica de ***host*** se encuentra descrito en RFC 2131. Para entrar en contexto, DHCP es un protocolo que permite asignar direcciones dentro de las organizaciones a los terminales que se puedan encontrar dentro de la red (PC, impresora, tabletas, etc.) de manera dinámica, haciendo más fácil la administración de la red. Al implementar un servidor DHCP en dichas organizaciones se permite que la administración de las direcciones IP y su asignación sea por medio de un único servidor. Debido a esta propiedad, el protocolo DHCP brinda eficiencia.

DHCPv4

El protocolo DCHPv4 proporciona direcciones IPv4 e información a la red de manera dinámica, debido a que los usuarios de PC de escritorio abarcan gran cantidad de la red. DHCPv4 es un aliado a la hora de la administración por parte de los encargados de la red, permitiendo un ahorro en los tiempos de gestión. En DHCPv4 se pueden encontrar diversas maneras para realizar el proceso de asignación de direcciones, las cuales permiten flexibilidad en el proceso:

Abarcan
Rodear, contener o comprender algo.

- **Asignación manual:** se da de manera manual por el administrador de la red al usuario designado (cliente).

- **Asignación automática:** DHCP permite asignación automática de información de direccionamiento (dirección IP-máscara de subred-***gateway***). Para la configuración del servidor DHCP es necesario un bloque de direcciones (conjunto de direcciones) para la asignación a los clientes DHCP en una red.

- **Asignación dinámica:** este proceso consta del arrendamiento por parte de DHCPv4 enfocado a una dirección IPv4 de un grupo de direcciones en un tiempo definido por el servidor o cuando el cliente decida prescindir del servicio. Este método es el que tiene mayor grado de aceptación en la actualidad y es el que se manejará en esta asignatura. El encargado de la red tiene a cargo configurar los servidores DHCPv4. Mediante este proceso se establecen los tiempos en los que se va arrendar el servicio. Al vencer el servicio, el cliente solicita una nueva dirección; muchas veces se le asocia la misma dirección IPv4.

DHCP opera de manera cliente-servidor. Al momento de establecer la comunicación entre el cliente con un servidor de DHCPv4, este servidor arrienda la dirección IPv4 al cliente. Paso seguido, el cliente accede a la red por medio de la IPv4 arrendada. Finalizado el tiempo del arriendo, el cliente se pone en comunicación con el servidor para seguir o no con el arriendo. Esto garantiza que las direcciones que ya no están en uso sean entregadas.

Configuración del cliente DHCPv4

Para configurar el cliente DHCPv4 se tienen en cuenta cinco pasos básicos:

1. El primer paso se origina cuando el cliente envía un mensaje de difusión **DHCP-DISCOVER** con su dirección MAC para identificar servidores DHCPv4 disponibles.

2. **Detección de DHCP (DHCPDISCOVER):** cuando el mensaje DHCPDISCOVER llega a los servidores de DHCPv4, el cliente desconoce la dirección IPv4 durante el inicio del proceso. Este utiliza direcciones de difusión a nivel de capa 2 y 3 para relacionarse con el servidor.

3. **Oferta de DHCP (DHCPOFFER):** al momento de recibir el mensaje DHCPDISCOVER por parte del servidor, este guarda una dirección IPv4, la cual estará disponible para arrendar al cliente. Además, el servidor de DHCPv4 envía un mensaje DHCPOFFER al cliente que realiza la solicitud. A diferencia del mensaje DHCPDISCOVER, el mensaje DHCPOFFER se transmite como una unidifusión y, para resaltar, se implementa la dirección MAC de capa 2 del servidor como IP de origen y la dirección MAC de capa 2 asociada al cliente como destino.

4. **Solicitud de DHCP (DHCPREQUEST):** una vez el cliente recibe el mensaje DHCPOFFER del servidor, responde con un mensaje DHCPREQUEST, el cual se implementa en el origen o en la renovación del arriendo.

5. **Acuse de recibo de DHCP (DHCPPACK):** una vez el servidor recibe el mensaje DHCPREQUEST, corrobora la información del arriendo mediante un PING a la dirección designada, con la finalidad de cerciorarse de que no esté en uso. Después de realizado el PING, el servidor habilita una nueva entrada ARP para el arrendamiento del cliente y envía un mensaje DHCPPACK, el cual tiene carácter unidifusión. Al momento de recibir el mensaje DHCPPACK por parte del cliente, este analiza la información de configuración e inmediatamente encamina una búsqueda de ARP hacia la dirección designada. Si no presenta respuesta al ARP, el cliente determina que la dirección es válida y la toma como propia e inicia su implementación.

Configuración de DHCPv4

Paso 1: excluir direcciones IPv4

Mediante el comando ***ip dhcp excluded-address*** se les permite a los enrutadores excluir una o varias direcciones cuando se desea realizar la asignación a los clientes. Este parámetro se puede implementar cuando se quiera guardar direcciones de carácter estático a determinados ***host***s, como la dirección del enrutador. Configuración del comando:

```
R1(config)# ip dhcp excluded-address dirección-ip {dirección-ip-final}
```

Paso 2: configurar un pool DHCPv4

Mediante el comando ***ip dhcp pool {pool-name}*** se asigna un grupo de direcciones al servidor. Configuración del comando:

```
R1(config)# ip dhcp pool {pool-name}
```

Paso 3: configuración de tareas específicas

Es necesario tener configurados el conjunto de direcciones y el *gateway*. Para cumplir con este requisito se implementa el comando *network:*

R1(dhcp-config)# network dirección-ip {máscara /longitud-prefijo}. Se define el rango de direcciones disponibles.

Cuando se implementa el comando *default-router* se establece la puerta de enlace o *gateway del router*. Esta puerta de enlace es la que tiene mayor cercanía con los clientes. Este comando se implementa de la siguiente manera:

R1(dhcp-config)# default-router gateway

Otros comandos que se implementan en DHCPv4 son:

- La dirección IPv4 asociada al servidor DNS que se manifiesta para un cliente DHCPv4. El comando que se utiliza para DNS es:

  R1(dhcp-config)# dns-server dirección-ip

- El comando *domain-name dominio* se implementa para asignar un nombre al dominio. El comando que se utiliza para configurar el dominio es:

  R1(dhcp-config)# domain-name dominio

Verificación del servidor DHCPv4

Para verificar que la configuración del servidor DHCPv4 está de la mejor manera se utilizan los siguientes comandos:

- **R1# show running-config l section dhcp:** permite visualizar los parámetros asociados a DHCPv4.

- **R1# show ip dhcp binding:** permite detallar las relaciones entre la dirección IPv4 y la dirección MAC otorgadas por DHCPv4.

- **R1# show ip dhcp server statistics:** permite visualizar los mensajes de envío/recepción del ***router*** y llevar la contabilidad de los mensajes que se enviaron y se recibieron.

Configuración del cliente DHCPv4

En las organizaciones pequeñas y oficinas domésticas (SOHO) es necesario configurar clientes DHCPv4, esto se asocia de manera inteligente con el ISP. La configuración del cliente se debe implementar sobre la interfaz Ethernet del enrutador, la cual brinda acceso a un módem. El comando que permite esta configuración es:

SOHO
Small office home office: organización pequeña a nivel de hogar e institución con un número corto de empleados.

Router(config)# interface ethernet 0

Router(config-if)# ip address dhcp

Router(config-if)# no shutdown

Router(config-if)# end

Verificación del cliente DHCPv4

Para verificar que la configuración de cliente DHCPv4 está de la mejor manera se utiliza el siguiente comando:

Router# show running-config

DHCPv6

El *Dinamic host configuration protocol for* IPv6 (DHCPv6) es definido en RFC 3315. En él, las direcciones de unidifusión global se pueden configurar manual o dinámicamente. La forma dinámica tiene dos maneras de configuración:

1. **Configuración automática de dirección sin estado (Slaac):** los dispositivos alcanzan una dirección IPv6 de unidifusión global con la ausencia de un servidor DHCPv6. Slaac implementa dos tipos de mensajes: de solicitud y de anuncio de *router* ICMPv6, los cuales brindan direccionamiento a un servidor DHCP.

   - **Mensaje solicitud de router (RS):** este mensaje es transmitido a la dirección IPv6 (multidifusión – FF02::2) de los enrutadores que forman parte de la red.

   - **Mensaje anuncio de router (RA):** tiene como objetivo brindar información a los clientes configurados y aprender sus direcciones IPV6 de una manera automática. Este mensaje es transmitido a la dirección (multidifusión – *FF02::1)* a todos los dispositivos de la red. Cuando se desee transmitir un mensaje RA se debe habilitar el enrutamiento IPv6, lo cual se logra mediante el siguiente comando: ***Router*(config)# ipv6 unicast-routing.**

¡Importante!

Si se desea modificar el mensaje RA que proviene de una interfaz de un enrutador y manifestar qué DHCPv6 sin estado está en uso, se implementa el siguiente comando: Router(config-if)# ipv6 nd other-config-flag.

- **Configuración de un router como servidor DHCPv6 sin estado**

Existen varios pasos para configurar un enrutador como **servidor DHCPv6:**

1. **Habilitar el enrutamiento IPv6:** los parámetros son los siguientes:

   Router(config)# ipv6 unicast-routing.

2. **Configurar pool de DHCPv6:**

   Router(config-dhcpv6)# ipv6 dhcp pool {pool-name}.

3. **Configurar los parámetros del *pool:*** en el mensaje RA hay una información que el servidor de DHCPv6 sin estado no facilita al cliente, de manera que este servidor se puede configurar para que otorgue información, como, por ejemplo: la dirección del servidor DNS y el dominio. Los parámetros que permiten la configuración de DNS y el dominio son:

   Router(config-dhcpv6)# dns-server dns-server-address

   Router(config-dhcpv6)# domain-name {domain-name}

4. **Configurar la interfaz DHCPv6:** los parámetros que permiten la configuración de la interfaz DHCPv6 son:

   Router(config)# interface type number

   Router(config-if)# ipv6 dhcp server {pool-name}

   Router(config-if)# ipv6 nd other-config-flag

- **Configuración de un *router* como cliente DHCPv6 sin estado**

  Existen varios pasos para configurar un enrutador como cliente DHCPv6. El cliente DHCPv6 sin estado puede ser una PC personal, un ***smartphone*** o una tableta. El ***router*** designado como cliente basa su configuración en una dirección IPv6 ***link-local*** para intercambiar información mediante mensajes IPv6 (mensajes RS). A continuación, se enuncian cada uno de estos:

  Router(config)# interface g0/0

  Router(config-if)# ipv6 enable

  Router(config-if)# ipv6 address autoconfig

  Router(config-if)# end

- Verificación DHCPv6 sin estado

  Para verificar que la configuración de DHCPv6 sin estado esté configurada de la mejor manera se utilizan los siguientes comandos:

- **Router# show ipv6 dhcp pool:** visualiza el nombre del ***pool*** de DHCPv6 y sus características.

- **Router# show running-config:** detalla cada uno de los comandos implementados en la configuración.

- **Router# show ipv6 interface g0/0:** visualiza que el enrutador tiene ***stateless address autoconfig enabled*** (configuración automática de dirección sin estado habilitada), así como una IPv6 de unidifusión global.

- **Router# debug ipv6 dhcp detail:** visualiza mensajes DHCPv6 que fueron vinculados con el cliente y el servidor.

2. **Servidor DHCPv6 con estado:** el proceso es similar a la configuración de un servidor DHCPv6 sin estado.

   1. **Habilitar el enrutamiento IPv6:** el comando IPv6 unicast-routing habilita el enrutamiento IPv6, dicho comando no es indispensable a la hora de designar un servidor DHCPv6 con estado, pero es necesario a la hora de enviar mensajes RA.

      Router(config)# ipv6 unicast-routing.

2. **Configurar el pool de DHCPv6:** el parámetro ipv6 dhcp pool {pool-name} origina un ***pool***. A continuación, se detallan los parámetros de configuración de pool de DHCPv6:

   Router(config-dhcpv6)# ipv6 dhcp pool {pool-name}.

3. **Configurar los parámetros del *pool:*** el servidor de DHCPv6 con estado facilita la configuración pertinente de direccionamiento, así como parámetros adicionales. Mediante el comando ***address longitud/prefijo*** se determina el grupo de direcciones que otorgará el servidor. El parámetro ***lifetime*** se refiere al arrendamiento válido dado en segundos. Otro parámetro que maneja el servidor DHCPv6 con estado es el DNS y el dominio.

   Router(config-dhcpv6)# address prefix/length [lifetime valid-lifetime preferred-lifetime l infinite]

   Router(config-dhcpv6)# dns-sever dns-server-address

   Router(config-dhcpv6)# domain-name {domain-name}

4. **Configurar la interfaz DHCPv6: los parámetros que permiten la configuración de la interfaz DHCPv6 son:**

   Router(config)# interface type number

   Router(config-if)# ipv6 dhcp server {pool-name}

   Router(config-if)# ipv6 nd managed-config-flag

- **Configuración de un *router* como cliente DHCPv6 con estado**

  Los parámetros que se implementan en la configuración de un enrutador como cliente DHCPv6 con estado son: habilitar dentro de la interfaz *ipv6 enable,* lo cual permite asimilar una dirección *link-local* para transmitir mensajes RS y el parámetro de configuración de interfaz *ipv6 address dhcp,* que permite al enrutador un funcionamiento como cliente DHCPv6. A continuación, se enuncia el proceso de configuración de un ***router*** como cliente DHCPv6 con estado:

  Router(config)# interface g0/0

  Router(config-if)# ipv6 enable

  Router(config-if)# ipv6 address dhcp

  Router(config-if)# end

- **Verificación DHCPv6 con estado**

  Para verificar que la configuración de DHCPv6 con estado esté configurada de la mejor manera se utilizan los siguientes comandos:

  - ***Router#* show ipv6 dhcp pool:** visualiza el nombre del ***pool*** de DHCPv6 con estado y sus características.

  - ***Router#* show ipv6 dhcp binding:** detalla la relación que se forma entre las direcciones ***link-local*** y la asignada por el servidor.

  - ***Router#* show ipv6 interface g0/0:** visualiza la dirección IPv6 de unidifusión global en el enrutador del cliente.

BIBLIOGRAFÍA

Aznar López, A. (2005). ***La red internet. El modelo TCP/IP***. Madrid, España: Grupo Abantos Formación y Consultoría.

Bellido Quintero, E. (2014). ***Equipos de interconexión y servicios de red (UF1879)***. Málaga, España: IC Editorial.

Boronat Seguí, F. (2013). ***Direccionamiento e interconexión de redes basadas en TCP/IP: IPv4/IPv6, DHCP, NAT, encaminamiento RIP y OSPF***. Valencia, España: Editorial de la Universidad Politécnica de Valencia.

Carceller Cheza, R. (2013). ***Servicios en red***. Madrid, España: Macmillan Iberia S. A.

Castaño Ribes, R. J. (2013). ***Redes locales***. Madrid, España: Macmillan Iberia S. A.

Hallberg, B. (2007). ***Fundamentos de redes***. Madrid, España: McGraw-Hill Interamericana.

Hillar, G. C. (2004). ***Redes: diseño, actualización y reparación.*** Buenos Aires, Argentina: Editorial Hispano Americana S. A.

Íñigo Griera, J. (2008). ***Estructura de redes de computadores***. Barcelona, España: Editorial UOC.

Jiménez Camacho, R. (2014). ***Análisis del mercado de productos de comunicaciones (UF1869)***. Málaga, España: IC Editorial.

Martínez Yelmo, I. (2015). ***IPv6-Lab: entorno de laboratorio para la adquisición de competencias relacionadas con IPv6.*** Madrid, España: Universidad de Alcalá.

Molina Robles, F. J. (2014). ***Servicios de red e internet***. Madrid, España: RA-MA Editorial.

Moreno Pérez, J. C. (2014). ***Sistemas informáticos y redes locales***. Madrid, España: RA-MA.

Santos González, M. (2014). ***Diseño de redes telemáticas.*** Madrid, España: RA-MA Editorial.

Velte, T. J. (2008). ***Manual de Cisco®***. Madrid, España: McGraw-Hill Interamericana.

Esta obra se terminó de editar en el mes de Septiembre 2018
Tipografá BrownStd Light, 12 puntos
Bogotá D.C,-Colombia.

AREANDINA

Fundación Universitaria del Área Andina

MIEMBRO DE LA RED

ILUMNO