compAs
Grupo de capacitación e investigación pedagogica

Redes de computadoras

Alejandro Fabian Mero García
Cesar Armando Moreira Zambrano
Walter Zambrano Romero
Dannyll Michellc Zambrano Zambrano
Duglas Antonio Mendoza Briones
Leonardo Chancay García
Camilo Jacinto Coronel Escobar
Jaime Gabriel Espinosa Izquierdo

Redes de computadoras

© Alejandro Fabian Mero García
Cesar Armando Moreira Zambrano
Walter Zambrano Romero
Dannyll Michellc Zambrano Zambrano
Duglas Antonio Mendoza Briones
Leonardo Chancay García
Camilo Jacinto Coronel Escobar
Jaime Gabriel Espinosa Izquierdo
Docentes Universidad de Guayaquil.

Título del libro
Redes de computadoras

ISBN: 978-9942-33-598-2

Publicado 2022 por acuerdo con los autores.

Guayaquil-Ecuador

Cita.
Mero, A., Moreina, C., Romero, W., Zambrano, D., Mendoza, D., Chancay, L., Coronel, C., Esponosa, J. (2022) Redes de computadoras Editorial Grupo Compás.

@grupocompas.ec
compasacademico@icloud.com

compÁs
Grupo de capacitación e investigación pedagógica

El contenido y gráficos de este compendio han sido obtenido mayoritariamente del curso CCNA de la academia de CISCO, información complementada con información de sitios web que se establecen en las referencias bibliográfica.

Índice

Tabla de contenido

Organización de la lectura para el estudiante por semana del compendio

Semanas	Paginas
Semana 1	Página 2 -43
Semana 2	Página 44 - 49
Semana 3	Página 50 – 62
Semana 4	Página 63 - 79

Resultado de aprendizaje de la asignatura

Conocer los principios básicos, componentes, dispositivos, protocolos, estándares y demás elementos que intervienen en una red de comunicación.

REDES DE COMPUTADORAS

Unidad 1: **Fundamento de las redes de datos y arquitectura de red**

Resultado de aprendizaje de la unidad:

Reconocer los conceptos, terminologías y principios generales sobre redes de computadoras, así como la comprensión de los modelos de referencias OSI y TCP/IP aplicado en el proceso de comunicación establecida entre un extremo (origen) y su otro extremo (destino).

Recuerde que. - El modelo de referencia OSI es el modelo de red descriptivo propuesto por la ISO que constituye un marco referencial para la definición de arquitecturas de interconexión de sistema de comunicaciones.

Recuerde que. - El protocolo TCP/IP surgió en el proyecto DARPA en 1969 y en 1983 el conjunto de protocolos TCP/IP fue adoptado como estándar convirtiéndose en el protocolo de internet.

Tema 1: Introducción a las redes de datos

Redes

- *Es el conjunto de equipos y dispositivos que se encuentran interconectado entre si por un medio, sean estos cableado o inalambricos*

Los avances actuales en materia tecnológica han originado un despliegue exponencial en las TI; las empresas, organizaciones y la sociedad en general han generado que la interrelación de las comunicaciones se viabilice hacia la aplicación de la tendencia digital.

El papel fundamental de cualquier comunicación se basa en las redes de datos, mismo que se integran de diversos componentes que permiten su interoperabilidad entre los medios existente, gracias a la aplicación de estándares comunicacionales garantizan la conectividad desde un emisor hacia un receptor, creando el feedback.

El presente contenido facilita al colectivo estudiantil de la carrera conocer los fundamentos que se aplican a nivel de las redes de datos, que abarcan sus estándares, protocolos, topologías, arquitectura, diseño e instrumentos que le permitirán analizar/monitorizar el desempeño de las comunicaciones.

Para el presente compendio de estudio se ha establecido cuatro unidades de trabajo, se inicia con una introducción a las redes de datos comunicacionales donde se establecen aspectos generales e histórico de la evolución a nivel de hardware y software, las clasificaciones de redes y finalmente se analizará el modelo de referencia OSI, así como la arquitectura de red TCP/IP. La unidad II establece un análisis detallado de las dos primeras capas del modelo de referencia OSI que abarca la capa física y enlace de dato donde se conocerá el esquema de funcionamiento de las capas, sus protocolos y técnicas empleadas. La unidad III comprende el estudio de la capa de red y direccionamiento IPv4/IPv6 y finalmente se culmina con la capa de transporte del modelo OSI.

Evolución histórica de las redes de comunicaciones.

¿Qué es una red?

Una red es una estructura compleja que relaciona diversos componentes y elementos que se comunican entre sí a través de un medio, el objetivo es establecer flujos y trayectorias con la finalidad de que se permita la comunicación en entre varios puntos.

¿Qué es comunicación?

La comunicación es la interacción entre dos o más personas en el cual se transmite un mensaje por varios canales, generando el feed back entre emisor y receptor.

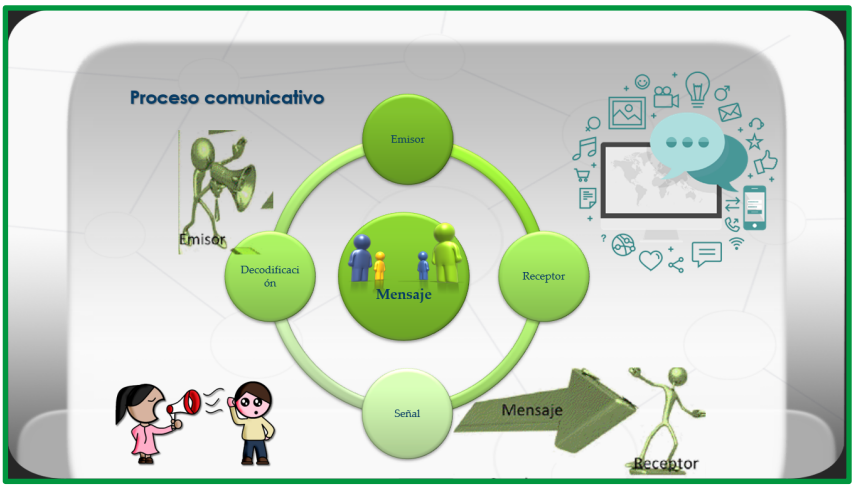


Figura 1: Proceso comunicativo

¿Historia de inicio de la comunicación?

La humanidad, desde sus inicios a establecido medios para comunicarse, se describen en resumen la panorámica del proceso de evolución y eventos que se generaron hasta llegar a la comunicación actual.

- **Prehistoria**: los primeros intentos del hombre de comunicación a distancia fueron extremadamente limitados: incendios, balizas, señales de humo, tambores de comunicación, bocinas.
- **Siglo VI a.C.**: al emperador persa Ciro el Grande se le atribuye haber establecido el primer sistema postal en la historia del mundo debido al descubrimiento de que las palomas tienen una extraña habilidad para encontrar su camino de regreso a sus nidos, independientemente de la distancia. Otras potencias antiguas como Egipto, Roma y China finalmente construyeron sus propios sistemas postales más adelante.
- **Siglo IV a. C.**: el semáforo hidráulico fue diseñado en la antigua Grecia como método de comunicación, y fue vital durante la primera guerra púnica.
- **Circa 490 a. C.**: la señal de heliógrafo o escudo se documentó por primera vez durante la famosa batalla griega de Maratón.
- **1041 – 1048**: Bi Sheng inventó en China donde ya existía un tipo de papel de arroz el primer sistema de imprenta de tipos móviles, que usaba complejas piezas de porcelana en las que se tallaban los caracteres chinos.
- **Siglo XV**: semáforo de bandera marítima: un código especial que involucra las posiciones de dos banderas de mano. Cada posición y movimiento representaba una letra o número. Esto facilitó la comunicación de las flotas.
  Nació la imprenta en la ciudad germana de Maguncia a mediados del siglo XV, de la mano de Johannes Gutenberg.
- **1672**: primer teléfono acústico mecánico experimental por Robert Hooke que descubrió que el sonido se podía transmitir por cable o cuerda a un auricular o boquilla conectados.
- **1729:** Stephan Gray descubre que la electricidad puede ser transmitida
- **1750**: Benjamin Franklin, con su famoso experimento de la cometa estableció la ley de conservación de la carga y determinó que debía de haber cargas positivas y negativas.
- **1780:** Charles Agustin de Coulomb midió fuerzas eléctricas y magnéticas utilizando una balanza de torsión que él mismo inventó
- **1790**: los hermanos Chappe crearon el primer sistema de telégrafo óptico utilizando el semáforo de la bandera marítima como punto de partida. Fue el primer sistema de telecomunicaciones en Europa
- **1801:** en la Academia de Ciencias de París ALEJANDRO VOLTA, físico italiano, presenta su invento llamado "pila de Volta".
- **1809:** el Alemán Samuel Thomas Soemmerring (1755-1830) inventó el telégrafo electro-químico cuyo principio se basaba en convertir agua en hidrógeno y oxígeno con electricidad.
- **1819**: Hans Crinstian Oersted encontró que un hilo por el que circulaba corriente hacía que se desviase una aguja imantada, demostrando que la electricidad podía producir magnetismo.Antes se consideraban fenómenos independientes.

- **1820:** André Marie Ampere, amplió las observaciones de Oersted, inventó una bobina consiguiendo la magnetización. Casi simultáneamente Georg Simon Ohm publicó su ley que relacionaba la corriente la tensión y la resistencia.
- **1831**: Michael Faraday demostró que un campo magnético variable podía producir una corriente eléctrica, utilizando para ello un imán en movimiento y viendo la corriente inducida en un hilo próximo.
- **1833-1837:** Carl Friedrich Gauss (1777-1835) y Wilhelm Weber (1804-1891) inventan varios telégrafos electromagnéticos. Weber realiza una conexión entre Göttinger Sternwarte y la Universidad con dos alambres.
- **1835**: Karl August Steinheil tratan de usar rieles para la transmisión de señales. El gran problema fue el aislamiento. 1840 La primera patente de Morse.
- **1842:** Joseph Henry, inventor de la telegrafía de hilos, demostró que con un circuito de descarga podía magnetizar agujas situadas en el sótano, dos pisos más abajo. Utilizando un hilo vertical detectó rayos a una distancia de unos 12 Km
- **1844**: en Estados Unidos, Samuel Findley Breese Morse construye la primera línea de comunicación telegráfica del mundo porque descubrió que cuando se conectan dos modelos de telégrafos y se pasa electricidad a través de un cable, se pueden enviar mensajes manteniendo presionados los botones en una serie de intervalos. Esto se conoció como el código Morse y sentó las bases para los teléfonos fijos modernos.
- **1849**: fue construida la primera línea de larga distancia para transmisión telegráfica entre Berlin y Frankfurt. Parte del cableado se hizo bajo tierra y el resto aéreo.
- **1850**: a través del cable marino se logra enlazar Inglaterra y Francia.
- **1851**: se instalaron las primeras alarmas de incendio por cable en Berlin y Munich por la firma Siemens & Halske.
- **1853**: se inventa el Telégrafo por cable para transmisión simultánea en ambas direcciones (modo dúplex), se usa el método de compensación, propuesto por el físico austriaco Julius Wilhelm Gintl
- **1858**: Cyrus Field de Nueva York colocó el primer cable transatlántico para conectar Inglaterra y los Estados Unidos por telégrafo.
- **1861**: Philip Reis demostró a varios profesores Alemanes su invento, el primer teléfono con posibilidad de transmisión de 90 metros, el uso una membrana animal excitada por un contacto eléctrico para producir sonidos, la recepción se lograba con un inductor galvánico oscilando de la misma forma que la membrana.
- **1866**: el primer cable submarino trasatlántico hace posible el telégrafo transatlántico entre EEUU- Francia.
- **1867**: Phillip Colomb ideó los primeros puntos y rayas se iluminaron con lámparas de señalización en el mar. Este código era similar al código Morse, pero finalmente, el código Morse se hizo más utilizado.
- **1873**: los experimentos de Faraday permitieron a James Clerk Maxwell, profesor de la Universidad de Cambridge en Gran Bretaña, establecer la interdependencia de la electricidad y el magnetismo. En su A treatise on Electricity and Magnetism publicó la primera teoría unificada electromagnética. Postuló que la luz era de naturaleza electromagnética y que era posible la radiación a otras longitudes de onda.

- **1874**: se inventa el Código de Emil Baudot utilizado en las primeras transmisiones telegráficas y radioeléctricas
- **1875:** Edison descubrió que las chispas de los interruptores eléctricos producían radiaciones, en 1885, patentó un sistema de comunicaciones utilizando antenas monopolo con carga capacitiva.
- **1876:** el 14 de febrero Alexander Graham Bell patenta el primer teléfono, este sistema estaba compuesto de micrófono y parlante, casi al mismo tiempo Elisa Gray patenta el micrófono.
- **1877**: se instala la primera Línea telefónica en Boston Sommerville
- **1878**: se instala la primera central Telefónica en New Haven, EEUU, constaba de un cuadro controlador manual de 21 abonados.
- **1880:** Tomas Alva Edison descubre, en una lámpara de incandescencia, el fenómeno de emisión en un filamento caliente.
- **1882**: Nikola Tesla construye un sistema de potencia alterna AC para reemplazar los generadores y motores de corriente directa (DC) que se encontraban en uso.
- **1883**: Edison descubre el llamado "efecto Edison" sobre el que se basa la electrónica moderna.
- **1884**: el investigador italiano Temístocles Calzecchi Onesti establece los fundamentos científicos del cohesor.
- **1886**: los datos para procesamiento del censo de EEUU son almacenados en tarjetas perforadas.
- **1887-1888**: H. Hertz probó la validez de las teorías de Maxwell. Para su experimento Hertz utilizó un dipolo alimentado en su centro con las descargas de una bobina. Como antena receptora usó una espira cuadrada con un entrehierro en el que se producían descargas. Hertz consiguió sintonizar el sistema añadiendo esferas a los brazos del dipolo, equivalentes a carga capacitiva y bobinas serie y condensadores paralelos a la espira receptora.
- **1891**: el físico francés Edouard Branly construyó el primer receptor de ondas electromagnéticas al que denominó cohesor. Consistía en un tubo lleno de limaduras de hierro conectado a una pila y un galvanómetro.
- **1892**: se logra el primer intercambio telefónico automático usando marcación sin operadora.
- **1894**: el Italiano Marconi efectúa la transmisión de señales inalámbricas a través de una distancia de 2 millas. El sabio inglés LODGE, en el Real Instituto de Londres, utilizando un excitador HERTZ y un cohesor Branly, establece la primera comunicación en morse a 36 metros de distancia.
- **1895**: el profesor ruso de matemáticas de la Universidad de Kazán, Alejandro Popoff, inventa la antena que asoció al tubo de limaduras de Branly para detectar tormentas lejanas. El ingeniero italiano Guillermo Marconi realiza su primer experimento de transmisión de señales radioeléctricas a poca distancia. Marconi transmite señales Morse, sin ayuda de alambre de unión, a una distancia de milla y media.
- **1896**: Marconi patenta un dispositivo de perfeccionamiento en las transmisiones de impulsos y señales eléctricas. con lo que se evoluciona a la radiotelegrafía

- **1897**: Oliver J. Lodge patenta una serie de importantes avances: los dipolos bicónicos, las cargas inductivas y la sintoiúa con circuitos resonantes.
- **1897**: se instala la primera estación Marconi en la isla Wight.
- **1898**: el 3 de junio Marconi inaugura el primer servicio radiotelegráfico regular entre Wight y Bournemouth, de 23 km. de distancia. Se constituye en Londres la primera sociedad telegráfica, The Wireless Telegraph & Signal Co., siendo nombrado Marconi su director para explotar la telegrafía sin hilos.
- **1899**: el día 28 de marzo Marconi asombra con la primera comunicación por radio entre Inglaterra y Francia a través del Canal de la Mancha. Las primeras palabras fueron para Branly, descubridor del cohesor.
- **1889**: las agrupaciones de antenas fueron propuestas por Sydney George Brown y James Erskine-Murray, aunque los primeros experimentos no se produjeron hasta 7 años después. Las antenas de' microondas, como reflectores parabólicos, lentes, bocinas y guías de onda ya se usaron antes de 1900.
- **1899**: primera central automática en Princentown EEUU
- **1901**: Marconi estableció la primera -comunicación transoceánica entre Cornualles en Gran Bretaña y Terranova, en Canadá. La frecuencia utilizada fue 820 KHz (366 m). La potencia del transmisor eran 15 kW. La antena transmisora era un monopolo en abanico, soportado por dos mástiles de 48 m separados 60 m. La antena receptora fue un hilo metálico, suspendido de una cometa.
- **1902**: Pousulen inventa su generador de arco que durante muchos años se utilizó en las emisoras de telegrafía sin hilos. Comunicaciones radioeléctricas para embarcaciones que navegaban alrededor del mundo usando código Morse.
- **1904**: John Ambrose Fleming, colaborador de Marconi, utilizó por primera vez una válvula termoiónica para detectar señales de radio.
- **1903**: se produce la primera comunicación con un buque de pasajeros, el "LUCIANA", desde las bases de Poldhu y Grace Bay.
- **1905**: las antenas habían evolucionado hacia un monopolo piramidal con carga capacitiva, a 70 KHz, en el lado británico y una estructura capacitiva con 200 radiales, a una altura de 60 m, en Terranova.
- **1906**: se construye en América el primer sistema para transmisión de voz a través de ondas electromagnéticas. Comienzo de la era Electrónica: rectificadores, triodos, válvulas termoiónicas, amplificadores, etc.
- **1906**: Marconi midió el primer diagrama de radiación de una antena de hilo paralela al suelo. Dicha antena es la precursora de las actuales antenas de onda progresiva, rómbicas y V.
- **1907**: Fleming perfecciona su diodo termoiónico detector de radio.
- **1908**: Lee de Forest, premio Nóbel de Física, construye el triodo. Permitió el desarrollo de amplificadores de radiofrecuencia, osciladores moduladores y la mejora de los receptores al combinar las válvulas con los circuitos resonantes.
- **1909**: intercambio telefónico automático entre Berlin y Munich (Alemania)
- **1910 – 1919**: se caracteriza por la construcción de transmisores con grandes antenas de baja frecuencia y elevada potencia. En la década 1910-1919 también se introdujeron

nuevas técnicas, como las ayudas a la navegación, las comunicaciones con submarinos sumergidos y los sistemas de control a distancia. Nace la transmisión AM, usando una frecuencia portadora modulada por una señal de voz.

- **1911**: se construyó las antenas de Radio Virginia, en Arlington, a la frecuencia de 137 KHz., El transmisor tenía una potencia da lOO kW.
- **1910**: se inventa el tubo de Vacuum, dispositivo que permite transmitir voz a través de largas distancias y más de una conversación sobre el mismo cable.
- **1913**: Meissner fabrica el primer oscilador.
- **1914**: en Estados Unidos se funda la A.R.R.L. (American Radio Relay League), primera organización de Radioaficionados de este País.
- **1915**: la Compañia De Telegrafos Del Oeste (EE.UU.) transmite la palabra por radiotelefonía desde Vermont a San Francisco, Hawai y París.
- **1916**: Marconi realizó una serie de experimentos con señales de 2 y 3 m de longitud de onda, utilizando reflectores parabólicos cilíndricos, construidos con hilos verticales. Los resultados de la experiencia aconsejaron la utilización de frecuencias de HF e impulsaron el descubrimiento de los enlaces troposféricos en 1932. Durante 1916 hubo emisiones diarias de música en New Rochele, en el estado de New York.
- **1918**: Armstrong proyectó el circuito superheterodino, básico para receptores AM (moduladores de amplitud).
- **1919**: se descubre la memoria binaria (conmutador) construido con dos triodos. El técnico investigador David Sarnoff, de la RCA, presenta a la dirección comercial y a los técnicos de esta compañía su proyecto del primer receptor de radio para uso público, siendo rechazado por unanimidad por no considerarlo rentable.
- **1920**: la emisora MARCONI WIRELESS de Chelsford (Inglaterra) transmite, en plan de ensayo el primer concierto de música clásica. La primera transmisión publica de radio toma lugar el 22 de diciembre en Koenigs-Wursterhausen – Alemania. Aparece la venta al público la revista "QST", órgano oficial de la A.R.R.L. de los EE.UU. En Pittsburgh (EE.UU.) se inaugura la emisora KDLA, que es la primera que emite programas regulares de radio. Amstrong desarrolla el circuito superheterodino.
- **1921**: la T.S.F. inicia en París los primeros ensayos de programas de radio para el público utilizando la Torre Eiffel como antena.
- **1922**: la BBC emitió su primer programa no experimental en noviembre. En España, la primera emisora fue Radio Barcelona, inaugurada en el 24 de octubre de 1924. En 1925 ya existían unos 600 emisores de ondas medias.

Las primeras antenas de radiodifusión eran muy similares a las utilizadas para las comunicaciones punto, a punto, pero pronto evolucionaron hacia el radiador de media onda, que ofrecía la ventaja de la cobertura omnidireccional.

Los receptores superheterodinos, inventados pro Edwin H. Armstrong, fueron posibles gracias a los tubos electrónicos. Los receptores utilizaban como antenas la red eléctrica y como masa las cañerías de agua, pero pronto evolucionaron hacia las antenas en forma de T y piquetas de masa.

- **1922**: Taylor y Young, del Naval Research -Laboratory (NRL), detectaron objetos en movimiento, midiendo las interferencias producidas en un sistema de radio de onda continuara la longitud de onda de 5 m con el transmisor y receptor separados, presagiando los sistemas de radar Propusieron continuar los trabajos, pero su plan no fue aceptado.
- **1923**: se instala la primera central telefónica de larga distancia (Bavaria, Alemania). Vladimir Zworykin patenta su invento el tubo de rayos catódicos usado más adelante como el principal elemento para la televisión. Los radioaficionados FRED SCHENELL (1MO), en América, y LEON DELOY (8AB), en Francia, establece una comunicación en la banda de 110 metros. Zworykin inventa el tubo para transmisión de señales de televisión.
- **1924**: radioaficionados realizan los primeros QSO entre Francia y Australia. El día 23 de marzo a las 10 de la noche comienzan las primeras emisiones experimentales españolas de radio en Onda Media desde el madrileño Prado del Rey n.18-22 a través de RADIO IBERICA, EAJ-6, que se inauguraría el día 12 de mayo a las diez de la noche.
- **1925**: Breit y Tuve midieron la altura de la ionosfera, utilizando para ello un radar pulsado.
  Los primeros experimentos de televisión se iniciaron en Gran Bretaña. En 1925 john Logie, Baird presentó un sistema de exploración mecánica de las imágenes.
- **1926**: en París se funda la I.A.R.U. (International Amateur Radio Union).

  Se descubre la Modulación en frecuencia (FM) con lo que se logra alta calidad del sonido para la radiodifusión.

  En **1926** UDA realizó las agrupaciones de un solo elemento activo, con elementos parásitos. Dichas antenas denominadas "Yagi", fueron dadas a conocer por el japonés así llamado, en un artículo publicado en inglés en el año 1928.

- **1927**: primer enlace continental mediante radio de onda corta
- **1928**: el físico alemán Paul Nipkow, inventor de la televisión realiza la primera transmisión inalámbrica de imágenes
- **1929**: Franklin desarrolló un radiofaro en Escocia. Se empezó a utilizar el sistema de búsqueda de dirección (DF) de Adcok consistente en cuatro monopolos. En 1928 Diamond y Dunmore desarrollaron el primer sistema de aterrizaje instrumental ILS.
- **1930-1939**: desarrollo de las microondas y el RADAR
  - **1930:** Walter Schottky y otros físicos descubrieron el mecanismo de los semiconductores, se inventó el LED, rectificadores y celdas fotovoltaicas. El físico alemán Fritz Schoter patento un sistema que mejoraba la calidad de video.
  - En el año **1930** se detectó, por primera vez un avión en vuelo, de una forma accidental. L. A. Hyland del Naval Research Laboratory (NRL). Comprobó, mientras probaba un sistema DF (direction finding), que, al pasar un avión por las cercanías, se producía un incremento en la señal recibida.
  - **1931:** primera transmisión electrónica de imágenes de televisión en Berlín. Allen Dumont inventa el osciloscopio.
  - En el año 1931 se estableció un enlace entre Francia y Oran Bretaña utilizando antenas reflectoras a 1760 MHz. Marconi midió el alcance sobre el mar de una

transmisión a 500 MHz, sobre el Mar Mediterráneo, encontrando que se podían recibir señales a una distancia igual a cinco veces el alcance visual, descubriendo lo que se conocería después como enlaces troposféricos.

- **1932**: los laboratorios de la A.R.R.L., en EE.UU., sale el prototipo del receptor superheterodino de JAMES LAMB. El día 26 de septiembre comienzan las emisiones experimentales de EAQ-MADRI, la primera emisora de radiodifusión en Onda Corta de España.
- **1932**: ya se había perfeccionado el sistema de radar en el NRL, y se podían detectar aviones a una distancia de 80 kilómetros del transmisor. Las primeras experiencias con un radar pulsado en EEUÚ se realizaron en el NRL, en abril de 1936, con un sistema a la frecuencia de 28.3 MHz y un ancho de pulso de 5 microsegundos. Al cabo de unos meses el alcance se aumentó en 40 Km.
- Pronto se llegó a la conclusión de que era necesario subir en frecuencia, especialmente para los sistemas embarcados. Los primeros sistemas a 200 MHz se empezaron a desarrollar en 1936. Con una potencia de 6 kW se alcanzaba una distancia de 50 millas. El sistema se denominó CXAM.
- **1935**: en Gran Bretaña se iniciaron los estudios sobre el radar cuando se propuso a Sir Robert Watson-Watt la construcción de un haz destructor con ondas de radio. Las conclusiones del estudio fueron de que no era viable, pero recomendaba estudiar el problema de la detección de objetos. En 1935 propuso las condiciones de funcionamiento. En 1936 se probó un sistema de interferencia de onda continua a 6 MHz. En 1935 se probó un sistema pulsado a 12 MHz, con un alcance de 40 millas.
- **1938**: se tenía en funcionamiento el famoso sistema de radar Chain Home, a, 25 MHz, con un total de 5 estaciones costeras.
- En Alemania se detectaron barcos en 1938 con un prototipo de radar llamado FREY A. La frecuencia de trabajo era de 125 MHz y el alcance entre 30 y 60 km. En otros países como Francia, Rusia, Italia y Japón también se hicieron experimentos de interferencia en sistemas de comunicaciones de onda continua, e incluso Francia y Japón instalaron sistemas que se revelaron poco útiles en general.

- **1930**: Radioastronomia, las interferencias que se producían en las comunicaciones de LF especialmente en el verano, hicieron que los laboratorios de la Bell encargaran a Karl G. Jansky , en 1930, un estudio para que determinara dichas direcciones, a fin de diseñar las antenas con nulos en ellas. Jansky construyó una antena tipo cortina de Bruce 8 elementos con reflector, funcionando en la banda de 14 metros, rotatoria. Con dicha antena comprobó que el ruido estaba originado en las tormentas, pero descubrió además una fuente de ruido que estaba siempre presente, y que tenía una periodicidad de 24 horas. Tras meses de observación Jansky determinó que provenía de la tierra y del sol y además que, había un ruido que provenía de la galaxia, con un máximo en el centro. Jansky había descubierto la Radioastronomía. Con las medidas del ruido se estableció el límite de sensibilidad que se podía alcanzar con un sistema receptor de onda corta.
  - **1938**: Grote Reber construyó una antena parabólica de 9 metros de diámetro, que funcionaba en la banda de 2 metros, con la que estableció los primeros radio

mapas del cielo. John D. Kraus descubrió en 1946, en la Universidad de Ohio State, la antena hélice. Se aplicó a la construcción de un radiotelescopio en 1951. La banda de funcionamiento era de 200 a 300 MHz.

- **1935**: se construyen los primeros cables coaxiales y multipar para propósitos de comunicación.
- **1936**: el ingeniero norteamericano ARMSTRONG desarrolla los estudios técnicos para la puesta en práctica de la FM. Fue desarrollado el primer modelo de calculadora programable "ZUSE Z1" por el ingeniero alemán Konrad Zuse, esta calculadora solo trabajaba con elementos mecánicos.
- **1936**: las primeras transmisiones experimentales de TV electrónica se realizaron durante los juegos Olímpicos de Berlín en 1936. Las emisiones regulares de la BBC comenzaron el mismo año. Se utilizaba la frecuencia de 45 MHz. La antena transmisora era una agrupación circular de dipolos.
- **1937**: es desarrollado el tubo Klyston Reflex para generación de señales de microondas.
- **1938**: el alemán Werner Flechsig (1900-1981) tiene la idea de construir los tubos de rayos catódicos a color.

- **1939-1945**: la segunda guerra mundial
  - La segunda guerra mundial supuso un esfuerzo considerable en el desarrollo de todas las tecnologías asociadas a las comunicaciones ya los sistemas de radar. Las investigaciones realizadas sentaron las bases para los desarrollos futuros de sistemas de aplicación civil.
  - Durante la segunda guerra mundial hubo un considerable esfuerzo en los sistemas de microondas, para aplicación a los sistemas de radar.
  - Se usaron los reflectores, lentes, bocinas, que ya se habían diseñado a finales del siglo XIX, para demostrar las teorías de Maxwell.
  - Durante esta época se utilizaron las guías de onda abiertas para alimentar reflectores o lentes, y las bocinas como radiadores poco directivos. También se desarrollaron las bocinas con dos modos para controlar la distribución de Campos en la apertura.
  - Se desarrollaron variaciones del reflector parabólico, como cilindros o sectores. Las antenas "pillbox" o "cheese" se inventaron durante los años de la guerra. Para conformar el haz en forma de cosecante se deformaron los paraboloides o se utilizaron múltiples alimentadores. Se diseñaron arrays de guías ranuradas, en la cara estrecha o en la cara ancha, con diseños resonantes o de onda progresiva. Durante la guerra se desarrolló toda la tecnología de guías de onda. Los trabajos de investigación fuerori recopilados posteriormente por el "Radiation Laboratory" , del M.I. T. , bajo la supervisión del "National Defense Research Coninúttee". Muchos de los textos siguen siendo una referencia obligada en la actualidad.
  - El magnetrón fue descubierto en el año 1940 en Gran Bretaña, por Boot y Randall. Dicho descubrimiento permitió el desarrollo del radar en ondas centimétricas. Se obtuvo una potencia media de 400 W utilizando un magnetrón de 6 cavidades, a la longitud de onda de 9.8 cm.

- En Estados Unidos se construyó el sistema EAGLE, con un array de 250 dipolos, a la longitud de onda de 3.2 cm, con la posibilidad de barrido en un margen de 60
- **1936**: la RBC inició la emisión de TV, utilizando sistemas mecánicos y electrónicos. Pronto se demostró la superioridad de los sistemas electrónicos. Durante la siguiente década se -demostraron las ventajas de aumentar el ancho de banda y la frecuencia (VHF).
- **1939**: la NBC comienza la difusión de señales de televisión comercial.
- **1940**: es instalado el primer servicio de radio teléfonos por "Deutsche Reichspost entre Berlín y New York.
- **1941**: se desarrolla la calculadora SUZE Z3 que incluía alrededor de 600 reles para cálculos y 2000 reles para memoria, trabajaba con el código binario "Leibnizsche. Son probados en USA los primeros programas de TV a color
- **1942**: inventado el casete para grabación magnética de audio.
- **1944**: en Estados Unidos Howard H. Aiken´s diseñó el primer computador programable llamado MARK1
- **1945**: Arthur C. Clarke, propuso en 1945 la utilización de los satélites geoestacionarios para los sistemas de comunicaciones de cobertura mundial. Un satélite en órbita circular ecuatorial de radio 42.242 vería siempre en la misma zona. Un satélite cubriría casi un hemisferio y con tres satélites espaciados 120 grados se tendría una cobertura mundial.

- **1946**: Radioastronomia, tras la segunda guerra mundial se produjo un resurgimiento de la radioastronomía. Se construyeron grandes instalaciones de observación. La primera de ellas fue la de Manchester (jodrell Bank) .En la actualidad d estacan varias instalaciones, como el de instituto Max Planck de radioastronomía, de 100 metros de diámetro y 3200 toneladas. Puede funcionar hasta 30GHz.

  Otra gran instalación es el reflector esférico fijo de 305 m de diámetro construido en Arecibo, Puerto Rico. El alimentador primario está soportado por cables y tres toues. Es posible un bauido de unos 20 grados desde el cenith.

  En San Agustín, Nuevo México se encuentra el array VLA (very large array), con 27 antenas cassegrain de 25 Km de largo que se pueden desplazar sobre tres ejes (separados 120 grados) de 21 Km de largo. Un radiointerferómetro de 5 km se encuentra en Cambridge.
- **1946**: Eckert y Mauchly desarrollaron la primera computadora totalmente electrónica conocida como ENAC, la cual contenía 1500 relés y acerca de 18000 tubos. El consumo de energía era de 150 kW, su peso de 30 toneladas aproximadamente y cubría un área de 140 metros cuadrados además era 1000 veces más rápida que MARK 1.
- **1946**: comenzó la gran expansión de la televisión. También Edwin H. Armstrong demostró la mejora de sonido en las transmisiones de radio, utilizando modulación de frecuencia en la banda de VHF.
- **1948**: los investigadores estadounidenses John Bardeen y Walter H. Brattain patentaron el transistor y B. Shockley los efectos del transistor como amplificador. El 1 de Julio la firma de los EE.UU. Bell Telephone Laboratories, anuncia por todos los medios de difusión norteamericanos el sensacional descubrimiento del transistor. Se definen regulaciones

telefónicas para uso de los teléfonos de marcación directa antes de la 2da guerra mundial, nace el conteo de duración de llamada por impulsos.

- **1947**-**RADAR**: Marcum y Swerhng presentan la teoría estadística de la detección. En 1953 Woodward propone la función de ambigüedad.
- **1949**: se inventan las primeras tarjetas de circuitos impresos con el fin facilitar la localización de los componentes y abaratar los costos de los equipos electrónicos.
- **1951**: Howard H. Aiken desarrolla el gran computador electromagnético
- **1954-RADAR**: se introduce la técnica M.T.1 para la visualización de blancos móviles.
- **1954**: se crea el primer radio-telescopio de 76 metros en Inglaterra.
- **1955**: se instala el primer sistema de marcación telefónica a larga distancia en Basel Suiza. Se descubre el diodo varactor.
- **1956**: Bell y Howel desarrollan la cámara de video electrónica.
- **1957-URSS**: fue lanzado al espacio el primer satélite por la URSS, era una esfera con un diámetro de 58 centímetros y un peso de 84 kilogramos, su nombre Sputnik
- **1958-EE. UU**: 18 de diciembre de 1958 se lanzó el SCORE (Signal Communicating by Orbiting Relay Equipment). La órbita era elíptica de baja altitud, con un período de 101 minutos. El satélite grababa el mensaje al pasar por una estación y lo reproducía frente a otra estación receptora. La longitud máxima del 'mensaje era de 4 minutos, equivalente a un canal vocal o setenta canales de teletipo de 60 palabras por minuto. La frecuencia del enlace ascendente era 150 MHz y el descendente de 132 MHz. Había -un radiofaro a 108 MHz. Las baterías del sistema fallaron a los 35 días.
- **1958**: desarrollo del circuito integrado. Primeras transmisiones de radio estereofónicas.
- **1960**: la NASA de EEUU puso en órbita a "Echo I A", el primer satélite de comunicaciones era una gran esfera metálica de 30m de diámetro localizada a una altitud de 1600 Km que reflejaba las señales radioeléctricas que recibía. Repetidor pasivo, sin ningún tipo de baterías o repetidores. Los períodos de rotación eran de 118 y 108.8 minutos. La órbita era muy baja, por lo que los satélites sólo eran visibles simultáneamente desde dos estaciones unos pocos minutos. La potencia de los -transmisores era de 10 kW, las frecuencias de 960 MHz y 2390 Ml4z, y las antenas de 25 y 18 m de diámetro.
- **1961**: IBM Alemania introduce el concepto de Tele-Procesamiento. Los datos transmitidos serial o paralelamente a través de una línea telefónica pueden ser reprocesados directamente en un computador. En el mes de diciembre es puesto en órbita el primer satélite artificial "OSCAR I" para el uso de los radioaficionados.
- **1962**: el 20 de mayo el satélite "TELSTAR I" puesto en órbita por 10 días, permite la primera transmisión de imágenes de televisión entre USA y Francia. Orbita baja, Primer satélite con repetidores de banda ancha 4/6 GHz.
- **1963**: TELSTAR II, lanzado en 1963.
- **1963**: desarrollado el Diodo Emisor de luz (LED).
- **1963**: primer mini-computador comercial.
- **1963-RADAR**: se publica la teoría del filtro adaptado, que ya se había usado durante el período de la guerra. En la década de los 60 se introducen las técnicas digitales.

- **1963-1964**: los satélites SVNCON II, y III fueron los primeros puestos en órbita geoestacionaria, en 1963 y 1964. El primero, de la serie falló durante el lanzamiento. La utilización era militar.
- **1964**: en USA el hospital de la Universidad de Nebraska, el Instituto Psiquiátrico de Omaha y el Hospital de Norfolk fueron enlazados por un canal de radio satelital empezando así la Telemedicina.
- **1964-EE. UU**: ECHO II lanzado el 25 de enero de 1964.
- **1965**: se logran las primeras fotografías del planeta Marte transmitidas desde el satélite Mariner 4.

Comunicación comercial vía-satélite – óptica

- **1965**: el primer satélite comercial en órbita geoestacionaria fue el INTELSAT I, también llamado Early Bird. Fue lanzado el 6 de abril de 1965 y estuvo en operación hasta 1969. Las comunicaciones se iniciaron de forma operativo el 28 de junio de 1965. El satélite tenía dos transpondedores de 25 MHz de ancho de banda. Los enlaces ascendentes estaban a 6301 MHz para Europa y 6390 MHz para Estados Unidos. Los enlaces descendentes estaban a las frecuencias de 4.081 MHz y 4161 MHz. Con dicho satélite se inicia la actual época de telecomunicación espacial.

  La organización INTELSAT inició sus actividades en 1964, con 11 países miembros, en la actualidad tiene 109 miembros y da servicio a 600 estaciones terrenas en 149 países. Las series de satélites van desde los INTELSAT I a INTELSAT VII.

  El INTELSAT I podía transmitir 240 canales vocales o un canal de TV.

- **1968**: los satélites de la serie INTELSAT III se empezaron a lanzar en 1968, podían transmitir 1200 circuitos telefónicos y 2 canales de TV.
- **1971**: los de la serie IV se empezaron a lanzar en 1971, con 4000 canales y 2 de TV.
- **1979**: se crea INMARSAT, organización internacional de satélites marítimos, y permite la comunicación a través de satélite con barcos. Se utilizan satélites MARECS.
- **1981**: la serie V se inicia en 1981, con 12000, canales vocales y 2 de TV. Finalmente los de la serie VI triplican la capacidad del anterior. Multiplica por 150 la capacidad del primer INTELSAT 1. El número de transpondedores es de 38, en la banda C y 10 en la banda Ku. Dichos satélites distribuían inicialmente la señal a las estaciones locales y redes de cable, pero en la actualidad pueden ser recibidos por usuarios individuales. Destacan los satélites europeos ECS y ASTRA, que trabajan en la banda de 10. 9 a 11.7 GHz y los satélites americanos en la banda de 3.7 a 4.2 GHz.
  Los satélites de difusión directa DBS tienen asignadas unas frecuencias diferentes, de 11.7 a 12.5 GHz, y podrán ser recibidos con antenas de diámetro reducido y receptores de bajo coste.
- **1966**: el científico Charles Kao de USA fue el primero en usar la luz a través de un conductor de fibra de vidrio para transmitir llamadas telefónicas.
- **1968-FAX**: la firma electrónica alemana Grundig introduce el concepto de Foto- telegrafía al permitir la transmisión de imágenes a través de líneas telefónicas.
- **1969**: Nacimiento de Internet, gracias al desarrollo de la red de computadores ARPANET.

- **1970**: se uso oficialmente el método de Multiplexación por división de tiempo (TDM) para intercambio telefónico.
- **1971**: Rank Xerox colocan la primera tele copiadora en el mercado. Desarrollo del microprocesador.
- **1971**: Raymond Tomlinson, inventa el correo eléctrico.
- **1972:** primeras 2839 conexiones de TV cable construidas en EEUU.
- **1974**: primera calculadora programable de bolsillo lanzada por Hewlett-Packard.
- **1975**: la compañía IBM desarrolla la primera impresora láser tipo IBM 3800, SONY saca al mercado el "Betamax", se inaugura en Toronto/Canada el TV más grande del momento (553.33 m).
- **1976**: SIEMENS desarrolla el teletipo, Motorola introduce la tecnología TTL para desarrollos de nuevos microprocesadores.
- **1977**: fue el año con mayor número de lanzamientos de satélites de comunicación (SIRIO I , CS , INTELSAT4), Siemens empezó la producción en masa de las centrales telefónicas EWS.
- **1978**: se logró tener información acerca de la atmósfera de Venus. Primera fibra óptica puesta en operación en Berlín.
- **1978**: el 3 de mayo, 600 usuarios de ARPANET recibieron el primer correo electrónico no solicitado, procedente de Gary Thuerk, director comercial de una empresa de informática estadounidense.
- **1979**: se introduce el servicio de Telefax en Frankfurt. SONY desarrolla el primer radio cassette. El 16 de julio se funda INMARSAT. Japonesa Matsushita Inc. patenta la pantalla de televisión de cristal líquido.
- **1980:** varias firmas japonesas lanzan al mercado los primeros receptores de radio sin condensador variable de sintonía, que es sustituido por un sintetizador PLL y un teclado numérico para marcar las frecuencias. Se incrementan las capacidades de almacenamiento en los microchips 64megas. Se posiciona en el mercado el primer computador portátil. Se introduce la tecnología de banda ancha para transmisión usando MHZ de BW. Se pueden realizar videoconferencias.
- **1981**: Finlandia, Suecia, Noruega y Dinamarca: sistema NMT (Nordic Mobile Telephone), 450MHz-.
- **1981**: se introduce la tecnología de sonido multicanal. Los primeros CD player y discos compactos se posicionan en el mercado.
- **1981**: primera red de telefonía móvil.
- **1982**: correo electrónico SMTP.
- **1982**: España, NMT a 450MHz
- **1982**: European Telecommunications Standards Institute (ETSI) establece un patrón común: El Groupe Special Mobile (GSM). Para una futura red celular de ámbito europeo.
- **1982**: el nuevo sistema de teletipo llamado Telefax se introduce en Alemania, Suiza y Gran Bretaña, tiene capacidad de procesamiento digital y velocidad de transmisión 1200 bit/s.
- **1983**: es el año de los computadores personales, discos flexibles y dispositivos de almacenamiento de información.

- **1983**: el sistema de nombres de dominio (DNS) fue probado por primera vez el 23 de junio de 1983 en la Universidad de Southern California, en Los Angeles (Estados Unidos).
- **1984**: por primera vez, imágenes de un cometa son transmitidas a la tierra por un satélite
- **1985**: se lanzan satélites para aplicaciones militares, aviones, mísiles etc...
- **1986**: la sonda Giotto se aproxima a 500 km del centro del cometa Halley y transmite datos físicos a la tierra
- **1987**: se empieza a utilizar el Nuevo formato de audio digital (DAT) donde la portadora de sonido excede en velocidad de grabación.
- **1987**: tecnología del GSM es Time Domain Multiple Access (TDMA).
- **1989**: sistemas de radiodifusión satelital digital en Alemania. Hay entones TV de alta definición. Con el Voyager 2 se capturan datos de 4.4 billones de kilómetros más allá del planeta Neptuno. Se establece el primer sistema de comunicaciones RDSI en el área de Rotterdam
- **1989**: Tim Berners-Lee, que trabajaba en 1989 en la Organización Europea de Investigación Nuclear (CERN), en la frontera entre Suiza y Francia, propuso "un sistema hipertexto distribuido" (la World Wide Web).
- **1990**: la comisión europea Rocket Ariane "localiza uno de los más grandes satélites de comunicación en el Eutelsat IIF1 con un peso de 1.8 toneladas y 16 canales que pueden soportar 17000 llamadas telefónicas o 16 canales de TV a color en el tráfico de datos.
- **1991**: Dockent 91-228 introduce los identificadores de llamada.
- **1991**: el Sr. Berners-Lee abrió el primer sitio web, en el cual explicaba el concepto de World Wide Web y su finalidad "de dar acceso universal a un gran universo de documentos". Ese mismo año se utilizó la primera webcam en la Cambridge University del Reino Unido.
- **1992**: nace Internet comercialmente
- **1992**: empieza a funcionar el GSM
- **1993**-**1998**: popularización de navegadores gráficos.
- **1993-1998**: los motores de búsqueda facilitan la navegación.
- **1994**: después de 25 años desde Arpanet, EEUU privatiza el manejo de Internet.
- **1996**: Terry Wynne da la idea del más grande proyecto en cuanto a redes a nivel mundial el www; se desarrolla el software para transmitir voz telefónica y música de alta calidad a través de Internet; es privatizada parcialmente Telefónica de España, lo que ha resultado de los mayores éxitos en la privatización de operadores públicos de telecomunicaciones.
- **1996-2007**: auge de la Web móvil e inicio de aplicación/desarrollo de teléfonos inteligentes.
- **1998**: sistemas de redes Ópticas pueden transmitir 3.2 Terabits por Segundo (equivale a 90.000 volúmenes de una enciclopedia). Crean el Chip DSL (Suscriptor de Línea Digital) que puede bajar datos a 1.5 megabits por segundo, 30 veces más rápido que los módems análogos.
- **1998**: teléfonos móviles satelitales de mano.
- **1999**: se declara en quiebra IRIDIUM el primer sistema de comunicaciones móviles de Tercera Generación, que iba a implantarse en el mundo.
- **1999**: Darcy DiNucci introduce el término web 2.0

- **2001**: la compañía DoCoMo lanza comercialmente la telefonía UMTS o de tercera generación en Europa.
- **2003**: las llamadas telefónicas ahora se podían transmitir a través de una computadora a través de protocolos de Internet. Nace la telefonía por internet VoIP.
- **2003 - 2005**: redes sociales e imágenes compartidas
- **2004**: Tim O'Reilly y Dale Dougherty profundiza el concepto de la web 2.0 en una conferencia.
- A partir de aquí, las comunicaciones sufren cambios, pero manteniendo las bases ya establecidas, pero que implican enormes avances científicos y tecnológicos. Se optimizan protocolos, medios de transmisiones, elementos y componentes que dan inicio a la era digital de la sociedad humana.

Figura 2: Evolución de las telecomunicaciones

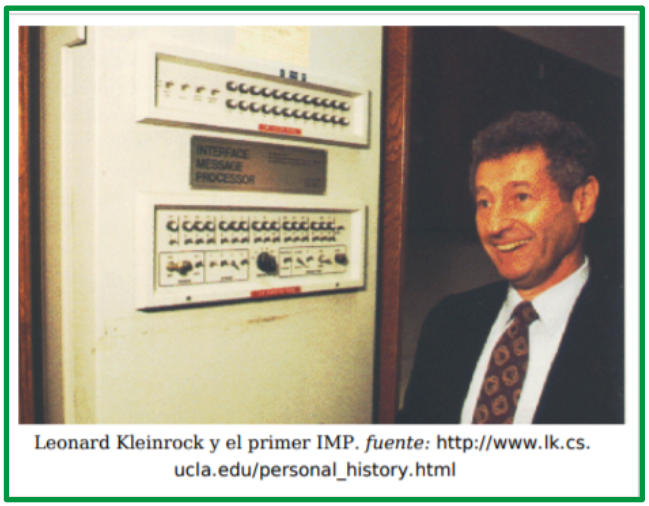
¿Qué es una red de computadora?

Una red de computadoras, es una red de ordenadores, de equipos comunicacionales y computacionales conectados por diferentes medios de transmisiones (cables, señales, ondas o cualquier otro método de transporte de datos) que comparten diferentes tipos de información, recursos y servicios.

Nacimiento de la red de computadoras (Internet)

La historia de Internet se remonta al temprano desarrollo de las redes de comunicación. La idea de una red de computadoras diseñada para permitir la comunicación general entre usuarios de varias computadoras se ha desarrollado en un gran número de pasos. La unión de todos estos desarrollos culminó con la red de redes que conocemos como internet. Esto incluía tanto desarrollos tecnológicos como la fusión de la infraestructura de la red ya existente y los sistemas de telecomunicaciones.

Un pionero fundamental en lo que se refiere a una red mundial, J.C.R. Licklider, comprendió la necesidad de una red mundial, según consta en su documento de enero, 1960, Man-Computer Symbiosis (Simbiosis Hombre-Computadora).



Leonard Kleinrock y el primer IMP. *fuente:* http://www.lk.cs.ucla.edu/personal_history.html

Figura 3: Precursor de la red mundial

En octubre de 1962, Licklider fue nombrado jefe de la oficina de procesado de información DARPA, y empezó a formar un grupo informal dentro del DARPA del Departamento de Defensa de los Estados Unidos para investigaciones sobre ordenadores más avanzadas. Como parte del papel de la oficina de procesado de información, se instalaron tres terminales de redes: una para la System Development Corporation en Santa Mónica, otra para el Proyecto Genie en la Universidad de California (Berkeley) y otra para el proyecto Multics en el Instituto Tecnológico de Massachusetts. La necesidad de Licklider de redes se haría evidente por los problemas que esto causó.

Como principal problema en lo que se refiere a las interconexiones está el conectar diferentes redes físicas para formar una sola red lógica. Durante los años 60, varios grupos trabajaron en el concepto de la conmutación de paquetes. Normalmente se considera que Donald Davies (National Physical Laboratory), Paul Baran (Rand Corporation) y Leonard Kleinrock (MIT) lo han inventado simultáneamente.

La **conmutación** es una técnica que nos sirve para hacer un uso eficiente de los enlaces físicos en una red de computadoras. Un Paquete es un grupo de información que consta de dos partes: los datos propiamente dichos y la información de control, en la que está especificado la ruta a seguir a lo largo de la red hasta el destino del paquete. Es importante señalar que el mensaje o trama de datos se fragmenta en otros paquetes, en la práctica, el tamaño típico de los paquetes TCP/IP suele ser de 1500 bytes.

Se puede dar como punto de partida del nacimiento de las redes de computadoras cuando en 1957 en los Estados Unidos crearon la Advance Research Projects Agency (ARPA), como organismo afiliado al departamento de defensa para impulsar el desarrollo tecnológico. La creación del ARPA, Leonard Kleinrock, investigador del MIT escribía el primer libro sobre tecnología basadas en la transmisión por un mismo medio de más de una comunicación.

Robert Taylor intentó hacer reales las ideas de Licklider sobre un sistema de redes interconectadas. Junto con Larry Roberts del MIT, inició un proyecto para empezar con una red similar. La primera conexión de ARPANET se estableció el 21 de noviembre de 1969, entre la Universidad de California, Los Ángeles y el Instituto de Investigaciones de Stanford. Antes del 5

de diciembre de 1969, se había formado una red de 4 nodos, añadiendo la Universidad de Utah y la Universidad de California, Santa Barbara. Usando ideas desarrolladas en la ALOHAnet, la ARPANET se inauguró en 1972 y creció rápidamente hasta el 1981. El número de hosts creció a 213, con uno nuevo añadiéndose aproximadamente cada 20 días.

ARPANET evolucionó usando estándares del proceso RFC, aún usado actualmente para proponer y distribuir protocolos y sistemas de Internet. El RFC1, titulado "Host Software", fue escrito por Steve Crocker desde la Universidad de California, Los Ángeles, y publicado el 7 de abril de 1969.

Las colaboraciones internacionales en ARPANET eran escasas; por varias razones políticas los desarrolladores europeos estaban preocupados en desarrollar las redes X.25, con la notable excepción del Norwegian Seismic Array en 1972 seguidos en 1973 por enlaces de los satélites a la estación terrestre de Tanum en Suecia y en la University College de Londres.

En 1965, la ARPA patrocino un programa que trataba de analizar las redes de comunicación usando computadoras. Mediante a este programa, la máquina TX-2 en el laboratorio Lincoln del MIT y la AN/FSQ-32 del System Development Corporation de Santa Mónica en California, se enlazaron directamente mediante una línea delicada 1200 bits por segundo.

En 1967, la ARPA convoca una reunión en Ann Arbor (Michigan), donde se discuten por primera vez aspectos sobre la futura ARPANET.

En 1968 la ARPA no espera más y llama a empresas y universidades para que propusieran diseños, con el objetivo de construir la futura red. La universidad de California gana la propuesta para el diseño del centro de gestión de red y la empresa BBN.

En 1969, año clave en las redes de computadoras, ya que se construye la primera red de computadoras de la historia, denominada ARPANET estaba compuesta por 4 nodos situados en UCLA (Universidad de California de Santa Bárbara, L.A), SRI (Stanford Research Institute), UCBS (Universidad de California de Santa Bárbara, L.A), UTA.

En 1970 la ARPANET comienza a utilizar para sus comunicaciones un protocolo Host-to-host. Este protocolo se denomina NCP y es el predecesor del actual TCP/IP que se utiliza en toda la Internet.

En 1971 la ARPANET estaba compuesta por 15 nodos y 23 máquinas que se unían mediante conmutación de paquetes. Ese mismo año Ray Tomlinson realiza un programa de e-mail para distribuir mensajes a usuarios concretos a través de ARPANET.

En 1972 se elige el popular @ como tecla de puntuación para la separación del nombre del usuario y de la máquina donde estaba dicho usuario. Hicieron una demostración pública y en esa misma demostración se realiza el primer chat.

En 1973 se produce la primera conexión internacional de la ARPANET. La conexión se realiza con el colegio universitario de Londres. La ARPANET contaba ya con 2000 usuarios y el 75% de su tráfico lo generaba el intercambio de correo electrónico.

En 1974, Cerf y Kahn publican un artículo, protocolo para interconexión de redes de paquetes, que especificaban con detalle el diseño del protocolo de control de transmisión (TCP).

En 1975, prueban los primeros enlaces vía satélite cruzando dos océanos (Hawai a Inglaterra) con las primeras pruebas de TCP de la mano de Stanford, UCLA y UCL.

A partir de la investigación del DARPA, las redes de conmutación de paquetes fueron desarrolladas por la Unión Internacional de Telecomunicaciones (UIT) en forma de redes X.25. X.25 formó la base de la red entre la academia británica y otros sitios de investigación en SERCnet, en 1974, que más tarde pasaría a llamarse JANET. El Estándar inicial de X.25 según la UIT se aprobó en marzo de 1976.

En 1978, la Oficina de Correos británica, Western Union International y Tymnet colaboraron para crear la primera red de paquetes conmutados internacional; refiriéndose a ella como "International Packet Switched Service" (IPSS). Esta red creció desde Europa y Estados Unidos hasta Canadá, Hong Kong y Australia antes del 1981, y pocos años después, creó una infraestructura de conexiones mundial.

Al contrario que ARPANET, X.25 estaba diseñado para poderse utilizar en oficina. Se usó para las primeras redes de teléfono de acceso público, tales como Compuserve y Tymnet. En 1979, CompuServe fue el primero en ofrecer posibilidades para el correo electrónico y soporte técnico a usarios de PCs. La compañía fue nuevamente pionera en 1980, como la primera en ofrecer chat con su CB Simulator. También estaban las redes de teléfono de America Online (AOL) y Prodigy, y varias redes BBS como The WELL y FidoNet. FidoNet era popular entre usuarios por hobby, parte de ellos hackers y radioaficionados

En 1979, dos estudiantes de la Universidad de Duke, Tom Truscott y Jim Ellis, propusieron la idea de usar scripts simples en Bourne Shell para transefir noticias y mensajes entre su universidad y la cercana Universidad de Carolina del Norte, Chapel Hill. Después de la salida del software al dominio público, la red de hosts UUCP usada para noticias Usenet se expandió rápidamente. UUCPnet, nombre que acabaría recibiendo, también crearía portales y vínculos entre Fidonet y los hosts de marcaje, telefónico BBS. Las redes UUCP se distribuyeron rápidamente debido a su bajo coste y a su capacidad de usar las líneas alquiladas ya existentes, los vínculos X.25 o incluso las conexiones de ARPANET. Antes de 1983 el número de hosts UUCP ya había aumentado a 550, casi duplicándose hasta los 940 en 1984.

El 27 de octubre de 1980 hubo una parada generalizada de la ARPANET da los primeros avisos sobre los peligros de la misma. Ese mismo año se crea redes particulares como la CSNET que proporciona servicios de red científicos sin acceso a la ARPANET.

En 1982, la DCA y la ARPA nombran a TCP e IP como el conjunto de protocolos TCP/IP de comunicación a través de la ARPANET.

Las redes basadas alrededor de ARPANET eran pagadas por el gobierno y por tanto restringidas a usos no comerciales tales como investigación; el uso comercial estaba estrictamente prohibido. Las conexiones se restringieron a sitios militares y universidades. En 1984 esto resultó en la primera red de banda ancha diseñada específicamente para usar TCP/IP. Esto creció como NSFNet, establecida en 1986, para conectar y proveer acceso a una cantidad de supercomputadores establecidos por la NSF.

En 1985 se establecen responsabilidades para el control de los nombres de dominio y así el ISI asume la responsabilidad de ser la raíz para la resolución de los nombres de dominio.

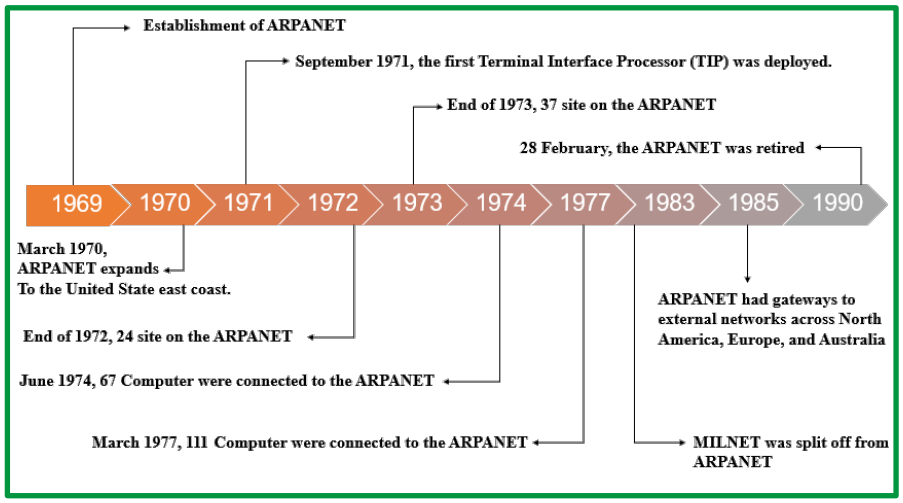


Figura 4: Proceso evolutivo de ARPANET

ARPANET empezó a fusionarse con NSFNet, originando el término Internet con, "una internet" definido como cualquier red que usase el protocolo TCP/IP. "La Internet" significaba una red global y muy grande que usaba el protocolo TCP/IP, y que a su vez significaba NSFNet y ARPANET. Hasta entonces "internet" e "internetwork" (lit."inter-red") se habían usado indistintamente, y "protocolo de internet" se usaba para referirse a otros sistemas de redes tales como Xerox Network Services. Como el interés en la expansión de las conexiones creció, y aparecieron nuevas aplicaciones para ello, las tecnologías de Internet se esparcieron por el resto del mundo. En 1984, University College London reemplazó sus vínculos por satélite transatlánticos por TCP/IP por medio del International Packet Switched Service (Servicio Conmutado de Paquetes Internacional).

Varios sitios que no podían conectarse directamente a Internet empezaron a hacerlo por medio de simples portales para permitir la transferencia de correo electrónico, siendo esta última por entonces la aplicación más importante. Esos sitios con sólo conexiones intermitentes usarían UUCP o Fidonet, y confiarían en los portales entre esas redes e Internet.

En 1984 Europa empezó a avanzar hacia un uso más general del TCP/IP, y se convenció al CERNET para que hiciera lo mismo. El CERNET, ya convertido, permaneció aislado del resto de Internet, formando una pequeña internet interna.

En 1988 Daniel Karrenberg, del Instituto Nacional de Investigación sobre Matemáticas e Informática de Ámsterdam, visitó a Ben Segal, coordinador TCP/IP dentro del CERN; buscando por consejo sobre la transición del lado europeo de la UUCP Usenet network (de la cual la mayor parte funcionaba sobre enlaces X.25) a TCP/IP. En 1987, Ben Segal había hablado con Len Bosack, de la entonces pequeña compañía Cisco sobre routers TCP/IP, y pudo darle un consejo a Karrenberg y reexpedir una carta a Cisco para el hardware apropiado. Esto expandió la porción europea de Internet sobre las redes UUCP existentes, y en 1989 CERN abrió su primera conexión TCP/IP externa. Esto coincidió con la creación de Réseaux IP Européens (RIPE), inicialmente un grupo de administradores de redes IP que se veían regularmente para llevar a cabo un trabajo

coordinado. Más tarde, en 1992, RIPE estaba formalmente registrada como una cooperativa en Ámsterdam.

En 1989, las universidades australianas se unieron al empujón hacia los protocolos IP para unificar sus infraestructuras de redes. AARNet se formó en 1989 por el Comité del Vice-Canciller Australiano y proveyó una red basada en el protocolo IP dedicada a Australia.

En Asia, habiendo construido la JUNET (Red Universitaria Japonesa) una red basada en UUCP en 1984 Japón continuó conectándose a NSFNet en 1989 e hizo de anfitrión en la reunión anual de The Internet Society, INET'92, en Kobe. Singapur desarrolló TECHNET en 1990, y Thailandia consiguió una conexión a Internet global entre la Universidad de Chulalongkorn y UUNET en 1992.

En 1992, se formó una sociedad profesional, la Internet Society (Sociedad de Internet), y la IETF se transfirió a una división de la primera, como un cuerpo de estándares internacionales independiente.

Componentes, dispositivos e interfaces de red

A continuación, se establecen los principales elementos de una red.

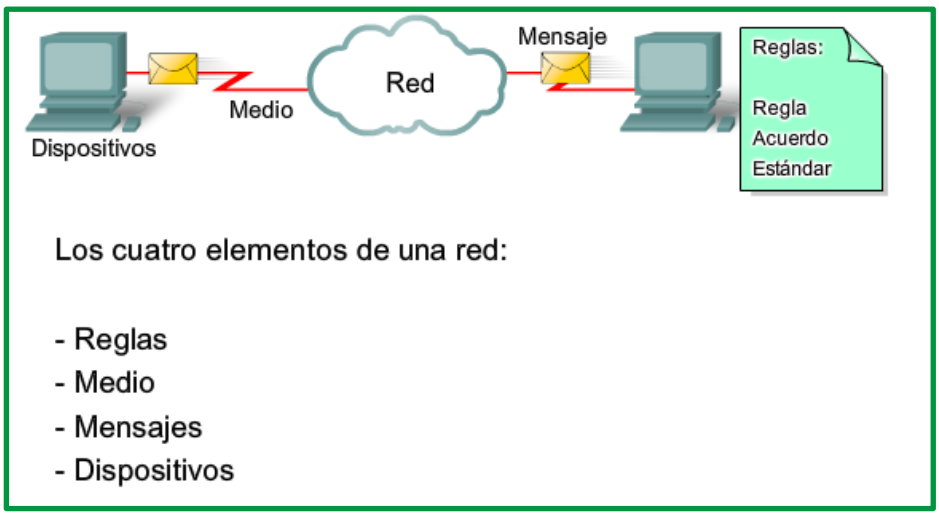


Figura 5: Principales elementos de una red

Dispositivos

Los dispositivos son todos aquellos componentes que permite la conexión de todos los ordenadores de la red. Dependiendo del tipo de red y del medio, se utiliza unos protocolos y servicios. Existen dispositivos de red y la elección de uno u otro depende del tipo de red, de la topología, de la funcionalidad para transmitir información desde un origen hacia un destino.

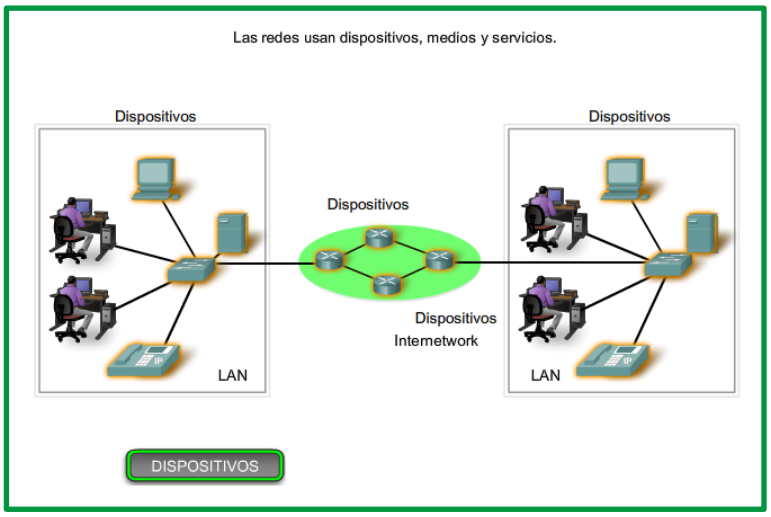


Figura 6: Dispositivos de redes

A nivel de red de comunicaciones se utiliza en simbología los siguientes dispositivos:

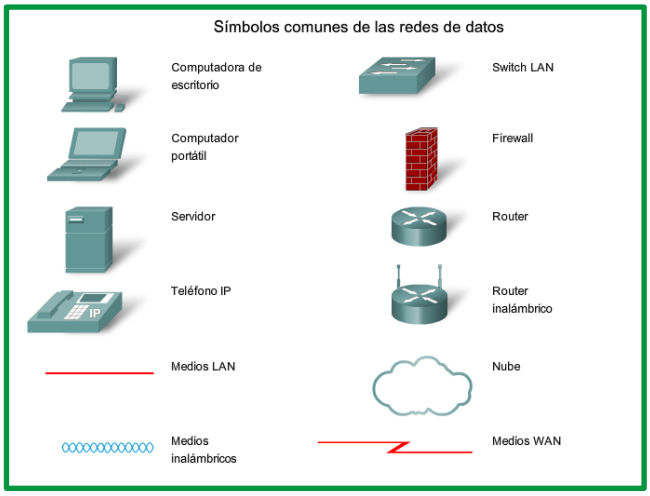


Figura 7: Símbolos comunes de los dispositivos de redes.

El TCP/IP, es el protocolo estándar usado a nivel mundial, los protocolos TCP/IP especifican los mecanismos de formateo, de direccionamiento y de enrutamiento que garantizan que nuestros mensajes sean entregados a los destinatarios correctos.

Mensaje.

El mensaje es la trama de datos (información) que viaja de un extremo otro por un medio de comunicación.

En la primera etapa del viaje desde origen al destino, el mensaje instantáneo se convierte en un formato que puede transmitirse en la red. Todos los tipos de mensajes tienen que ser convertidos a bits, señales digitales codificadas en binario, antes de ser enviados a sus destinos. Esto es así sin importar el formato del mensaje original: texto, video, voz o datos informáticos. Una vez que el mensaje instantáneo se convierte en bits, está listo para ser enviado a la red para su remisión.

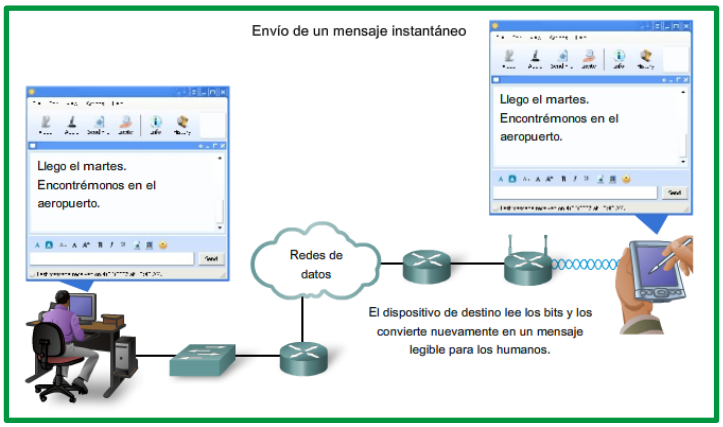


Figura 8: Aspectos en envió de un mensaje instantáneo

Un mejor enfoque para enviar datos a través de la red es dividir los datos en partes más pequeñas y más manejables. La división del stream de datos en partes más pequeñas se denomina segmentación. La segmentación de mensajes tiene dos beneficios principales.

Primero, al enviar partes individuales más pequeñas del origen al destino, se pueden entrelazar diversas conversaciones en la red. El proceso que se utiliza para entrelazar las piezas de conversaciones separadas en la red se denomina multiplexación.

Segundo, la segmentación puede aumentar la confiabilidad de las comunicaciones de red. No es necesario que las partes separadas de cada mensaje sigan el mismo recorrido a través de la red desde el origen hasta el destino. Si una ruta en particular se satura con el tráfico de datos o falla, las partes individuales del mensaje aún pueden direccionarse hacia el destino mediante los recorridos alternativos. Si parte del mensaje no logra llegar al destino, sólo se deben retransmitir las partes faltantes.

La desventaja de utilizar segmentación y multiplexación para transmitir mensajes a través de la red es el nivel de complejidad que se agrega al proceso. Supongamos que tuviera que enviar una carta de 100 páginas, pero en cada sobre sólo cabe una. El proceso de escribir la dirección, etiquetar, enviar, recibir y abrir los cien sobres requerirá mucho tiempo tanto para el remitente como para el destinatario.

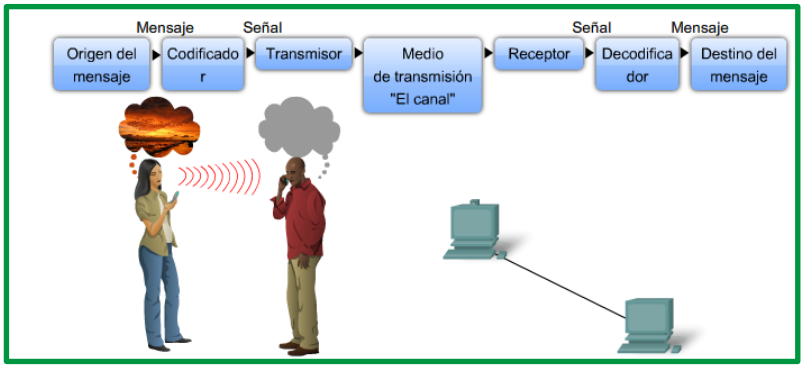


Figura 9: Proceso codificación/decodificación en envío de mensaje

Medio.

El medio es el que permite la comunicación del mensaje a través de cables o ondas electromagnéticas según sea el caso, los medios de transmisión se clasifican en medios de transmisión guiados y medios de trasmisión no guiados.

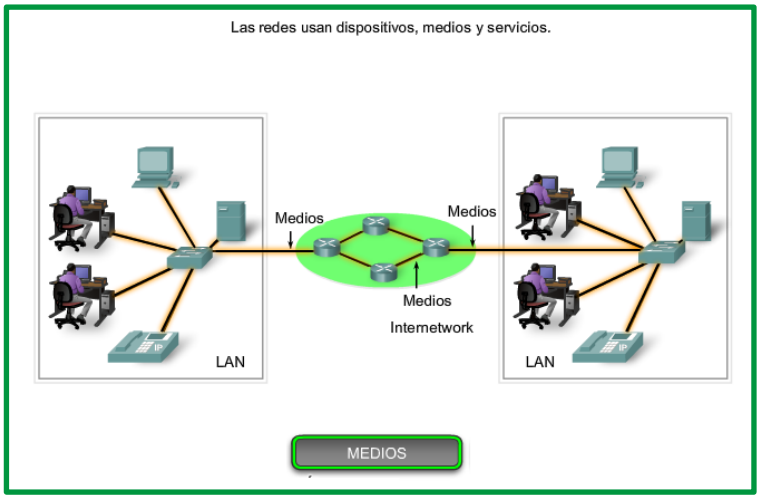


Figura 10: Medios utilizados para transmisión de datos en las redes LAN y WAM

Medios de transmisión guiados: Son aquello que se aplica en las comunicaciones un conductor físico desde un extremo al otro.

Par trenzado: Existen varios tipos de cables, se clasifican en Cable UTP, Cable FTP, Cable STP, Cable SSTP, Cable SFTP. Se detallan las principales características del cable par trenzado:

- Consiste en dos alambres de cobre aislados
- Se trenzan para reducir interferencias
- Es el medio de transmisión más usado
- Se agrupan para formar cables mayores
- Transmite tanto señal analógica como digital
  - Analógica: AB=250 KHz
  - Digital: V=100/1000 Mbps

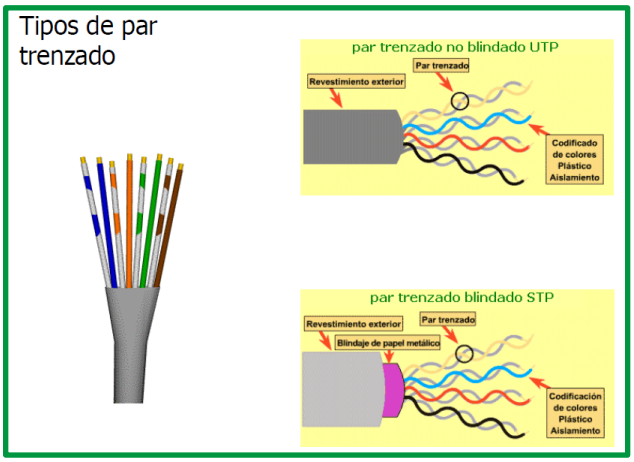


Figura 11: Tipos de par trenzado

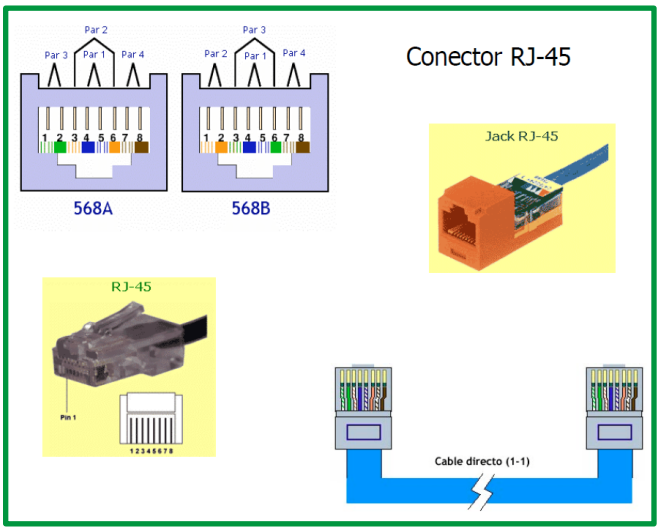


Figura 12: Conectores utilizados en par trenzado

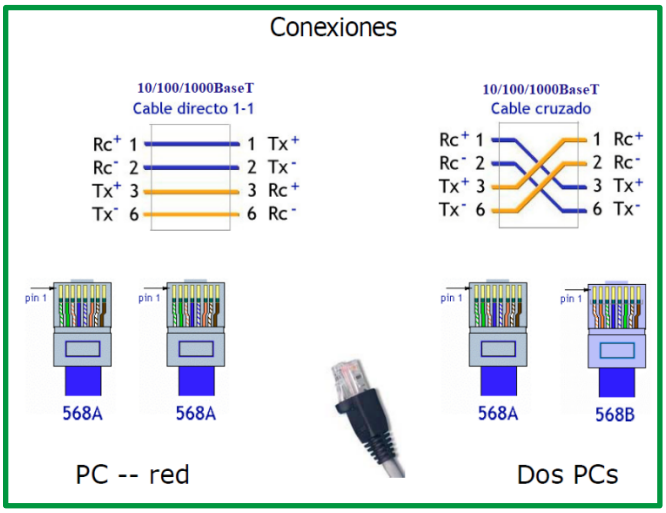


Figura 13: Conexiones en para trenzado

A continuación, se detallan las características de las categorías de cables dentro de las comunicaciones LAN, tenemos:

- **Cat 5.** Esta categoría no está actualmente reconocida por TIA/EIA, aunque todavía los podemos encontrar en instalaciones. Se usa en redes fast ethernet, hasta 100 Mbps y están diseñados para transmisión a frecuencias de hasta 100 MHz.
- **Cat 5e**. Está definido en TIA/EIA-568-B y soporta velocidades gigabit ethernet de 1000 Mbps. Está diseñado para transmisión a frecuencias de 100MHz, pero puede superarlos.
- **Cat 6.** Definida en TIA/EIA-568-B y usado en redes gigabit ethernet a 1000 Mbps. Han sido diseñados para transmisión a frecuencias de hasta 250 MHz.
- **Cat 6A.** Usado en redes 10 gigabit ethernet o 10000 Mbps. Funcionan a frecuencias de hasta 500 MHz.

- **Cat 7.** Suben el listón para funcionar a 600 MHz según la norma internacional ISO-11801 y se utilizan en redes 10 gigabit ethernet.
- **Cat 7A,** con frecuencias de 1000 MHz y conexiones de redes 10 gigabit ethernet.
- **Cat 8** es el nuevo estándar compatible con frecuencias 2000 MHz y velocidad de 40 Gbps o 40000 Mbps.

Coaxial: Sus principales características son**:**

- Alambre de cobre formado por núcleo y malla
- Buena combinación de ancho de banda e inmunidad al ruido
- Dos clases de cable coaxial
  - Cable de 50 ohm: digital
  - Cable de 75 ohm: analógico
- Se usa para televisión, telefonía a gran distancia, LAN, etc.

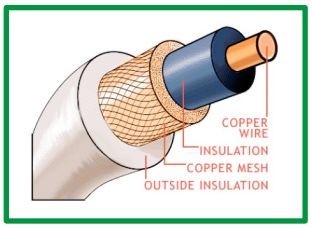


Figura 14: Cable coaxial

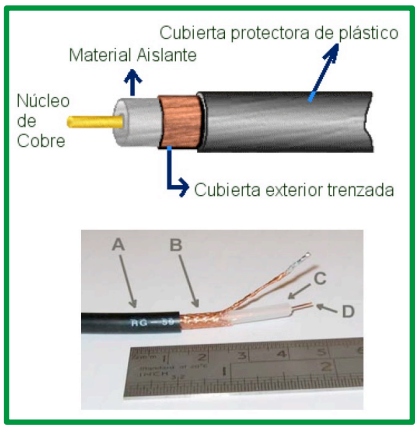


Figura 15: Componentes del cable coaxial

Fibra Óptica: Un cable de fibra óptica consta de tres secciones concéntricas. El núcleo, consiste en una o más hebras o fibras hechas de cristal o plástico, cada una de ellas lleva un revestimiento de cristal o plástico con propiedades ópticas distintas a las del núcleo. La capa más exterior recubre una o más fibras, debe ser de un material opaco y resistente.

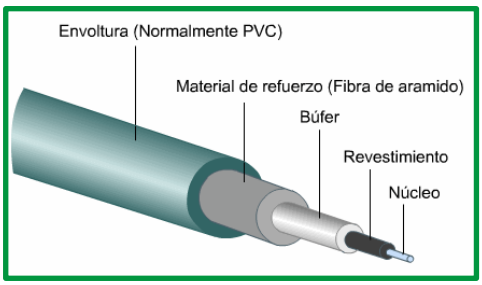


Figura 16: Componentes de la fibra óptica

Un sistema de transmisión por fibra óptica está formado por una fuente luminosa muy monocromática (generalmente un láser), la fibra encargada de transmitir la señal luminosa y un fotodiodo que reconstruye la señal eléctrica. Sus características son:

- Reflexión total

- Fibra multimodo

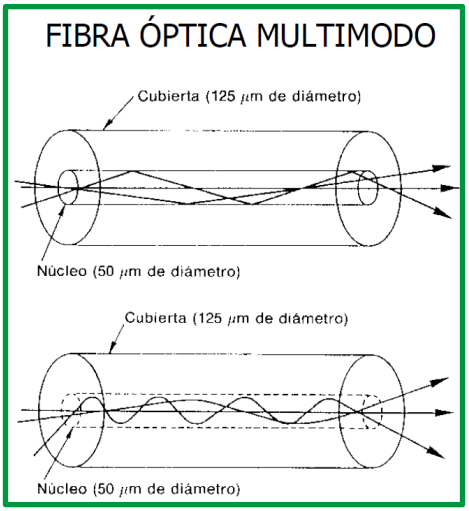


Figura 17: Fibra Óptica multimodo

- Fibra monomodo

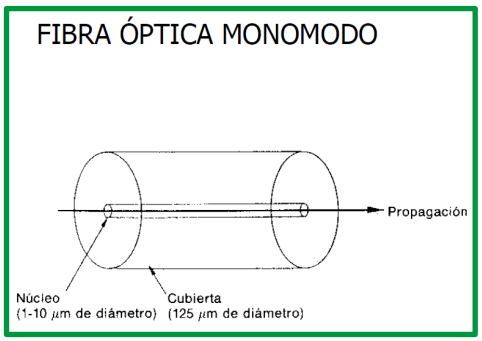


Figura 18: Fibra Óptica monomodo

- Presenta dispersión

Medios de transmisión no guiados

Los medios no guiados o comunicación sin cable transportan ondas electromagnéticas sin usar un conductor físico, sino que se radian a través del aire, por lo que están disponibles para cualquiera que tenga un dispositivo capaz de aceptarlas. Se detallan los principales medios de trasmisión no guiado.

Ondas de radio:

Las ondas de radio utilizan cinco tipos de propagación: superficie, troposférica, ionosférica, línea de visión y espacio. Cada una de ellas se diferencia por la forma en que las ondas del emisor llegan al receptor, siguiendo la curvatura de la tierra (superficie), reflejo en la troposfera (troposférica), reflejo en la ionosfera (ionosférica), viéndose una antena a otra (línea de visión) o siendo retransmitidas por satélite (espacio). Las bandas de frecuencias son: LF, MF, HF, VHF, UHF. (bandas cubren aproximadamente desde 55 a 550 MHz).

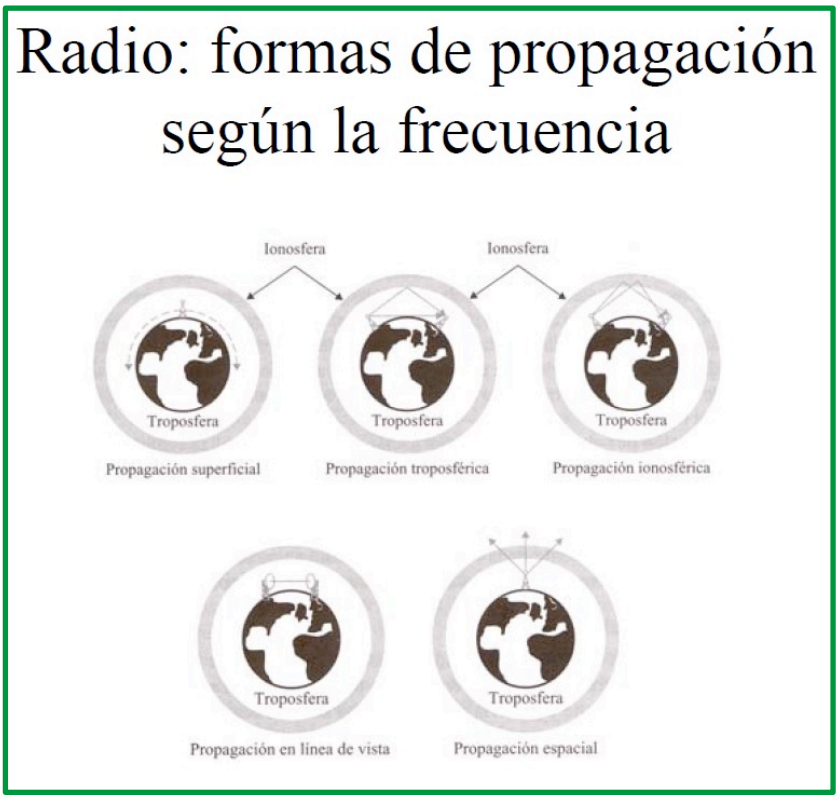


Figura 19: Formas de propagación de las ondas de radio según la frecuencia

Microondas

Las microondas nos permiten transmisiones tanto terrestres como con satélites. Dada sus frecuencias, del orden de 1 a 10 GHz, las microondas son muy direccionales y sólo se pueden emplear en situaciones en que existe una línea visual que une emisor y receptor. Los enlaces de microondas permiten grandes velocidades de transmisión, del orden de 10 Mbps.

Figura 20: Enlace microondas

Infrarrojos

Utilizan un haz de luz infrarroja que transporta los datos entre dispositivos. Debe existir visibilidad directa entre los dispositivos que transmiten y los que reciben ya que de lo contrario se puede ver interrumpida la comunicación. Existen 3 modos de transmisión:

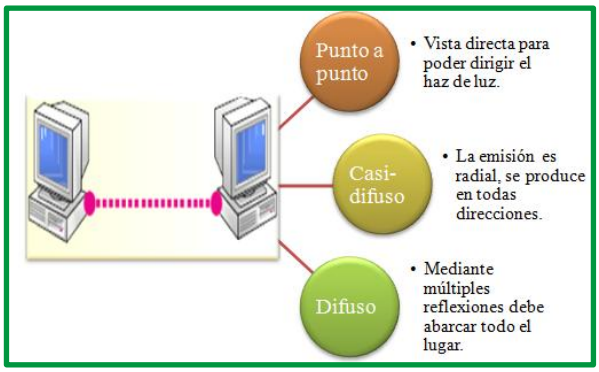


Figura 21: Comunicación Infrarroja

Ejemplo de comunicación infrarroja a corta distancia.

Figura 22: Ejemplo de comunicación infrarroja

Satélites

Los satélites reciben las señales y las amplifica o retransmite en la dirección adecuada. Para mantener la alineación del satélite con los receptores y emisores de la tierra, el satélite debe ser geoestacionario.

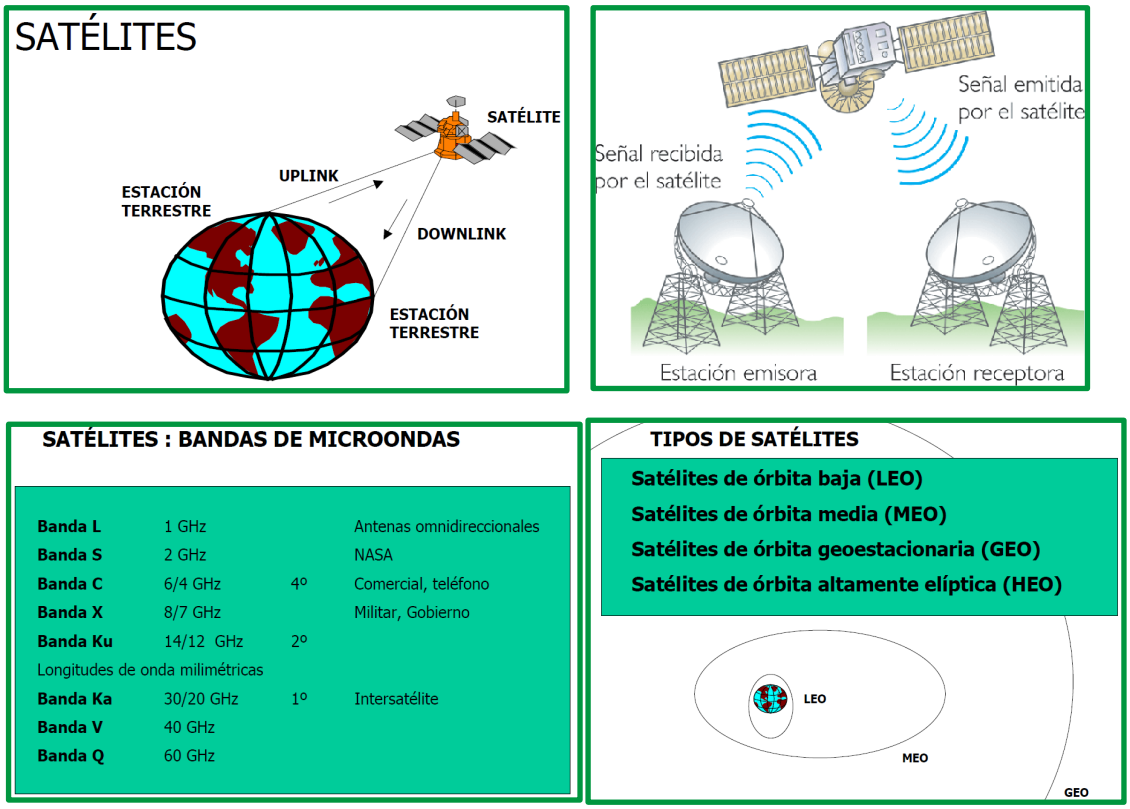


Figura 23: Elementos requeridos en una comunicación Satelital

Reglas:

Las reglas en las comunicaciones permiten establecer la comunicación entre dispositivos garantizando los procesos respectivos para **establecer**, **mantener**, **controlar** y **cerrar** conexiones; los métodos de comunicación establecen tres elementos: origen (emisor), destino (receptor) y canal (medio por el cual el mensaje viaje desde origen a destino). Los protocolos que se utilizan son específicos, sus características en el método de comunicación consideran el origen, el destino y el canal. Las reglas o protocolos, deben respetarse para que el mensaje se envíe y comprenda correctamente. Algunos de los protocolos que rigen con éxito las comunicaciones humanas son:

- Emisor y receptor identificados,
- Método de comunicación consensuado (cara a cara, teléfono, carta, fotografía),
- Idioma y gramática comunes,
- Velocidad y temporización en la entrega, y
- Requisitos de confirmación o acuse de recibo (ACK).

Servicios: es el conjunto de sistemas/aplicaciones que están definida básicamente por softwares misma que son abstracta para los usuarios finales, les brinda a los usuarios las capacidades de establecer comunicaciones entre si compartiendo y utilizando los diversos recursos disponibles en una red.

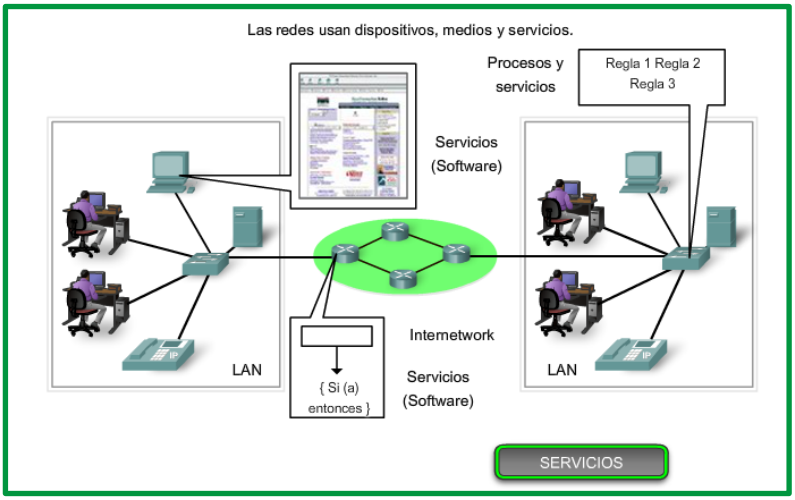


Figura 24: Elementos que intervienen en una red de datos

Dispositivos e interfaces de redes.

A nivel de redes de comunicaciones, intervienen varios dispositivos que cada uno cumplen con una función específica que está definida por el IOS (sistema operativo). Entre los principales tenemos:

Pasarela o Gateway: se utiliza para interconectar redes con protocolos y arquitecturas completamente diferentes a todos los niveles de comunicación, tienen poca velocidad de transmisión porque realizan proceso de conversión/traducción de unidades de información. Un ejemplo de su aplicación la coexistencia de líneas telefónicas análogas y digitales.

Router: es un enrutador de capa 3, ayuda a dirigir mensajes a medida que viajan a través de la red.

Switch: es un dispositivo de interconexión utilizado para conectar varios equipos/elementos en una red.

Firewall o **cortafuego**: es el disposotivos de hardware o un software que nos permite gestionar, filtrar y controlar el trafico entrante y saliente que se genera entre 2 o mar redes en una misma organizaciòn.

Router inalámbrico: es un dispositivo que realiza funciones de enrutador, pero incluye funciones de un punto de acceso.

Access Point: Punto de acceso inalambrico es un dispositivo de red que permite la interconexiòn equipos de comunicaciòn inalambrica a nivel local y de internet.

Modem: es un dispositivo que actua como encaminador que ofrece comunicaciones de alta velocidad para cortas distancias.

Hub: es un dispositivo concentrador que permite conectar varios equipos de red entre si bajo el mismo dominio de red.

Controladora Wifi: es un dispositivo que permite desplegar una red local inalámbrica que controla de forma centralizada un grupo de access point. Se permite configurar, monitoriza y diagnosticar los dispositivos conectados a la red inalámbrica.

Servidores: los servidores son los encargados de gestionar los servicios, recursos e información compartida dentro de una red, estos pueden ser servidores físicos que incluyan varios servidores a nivel de software (servidores: correo, impresión, archivos, web, entre otros).

Tarjeta de red: conocida como NIC, es un adaptador de red LAN que se aplica con medios guiados y medios no guiados.

Dispositivos finales: a los dispositivos de red que los usuarios están más familiarizados son las siguiente:

Terminales: son los computadores u ordenadores que se encuentra conectados a la red, se les conoce como nodo o estación de trabajo.

Laptop: es un computador u ordenador portátil que puede ser trasportada fácilmente.

Smart TV: son televisores inteligentes que permite actualmente realizar tareas que hasta ahora solo se realizaban con ordenadores.

Smartphone: son teléfonos inteligentes con pantalla táctil que combina las funciones de un celular y ordenador, tienen sistemas operativos que le permites realizar tareas que realiza un ordenados.

Impresora: son dispositivos que se comparte en una red de trabajo que permite realizar las impresiones de la información requerida por los usuarios.

Teléfonos IP: son teléfonos destinados a trabajar a través de centrales telefónicas digitales permitiendo realizar llamadas a través del internet o llamada de Voz IP, el estándar del protocolo usado es el SIP.

Tablet: es un deposito electrónico portátil de mayor tamaño que un teléfono inteligente.

Cámara IP: son dispositivos que emiten señales de video y audio a través de una red a una central donde se almacenan sus contenidos para su análisis y monitoreo en caso de requerírsele.

Interfaces de red TCP/IP: A nivel de una red, la comunicación de nodos o equipos requieren que se establezcan la interconexión a través de los medios de comunicación; los medios de comunicación realizan esta conexión por medio de interfaces.

Una interfaz de red, es el software específico de red permite que se comunique el controlador de dispositivo específico de red y la capa IP a fin de proporcionar a la capa IP una interfaz coherente con todos los adaptadores de red que puedan estar presentes.

A nivel general en las redes se establecen básicamente dos tipos de interface: Interfaces LAN e Interfaces WAN. Para conocimiento e ilustración se detalla en esquema lógico la interface de conexión de un router que trabaja a nivel de enrutamiento:

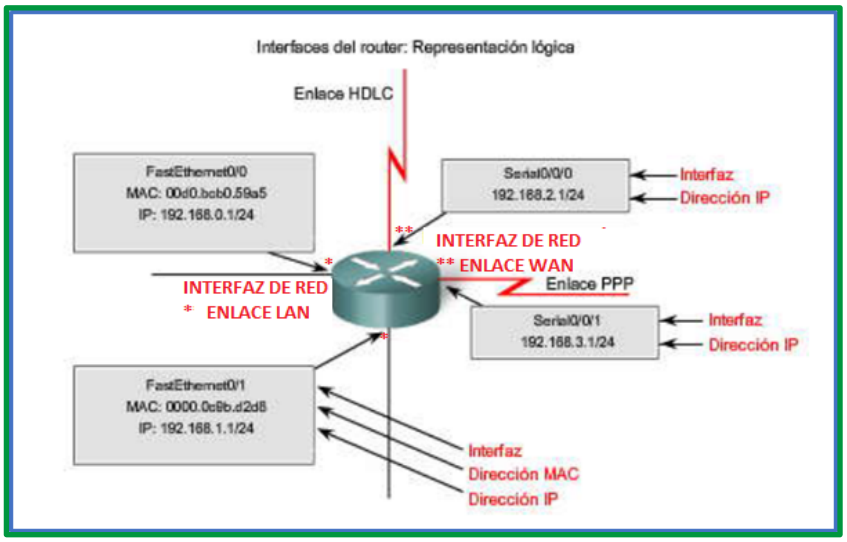


Figura 25: Interfaces del router (dispositivos de red)

Es importante señalar que cada dispositivo de red se compone de diferentes interfaces de redes, interfaz que depende de la función que desempeñan o cumple en una red de comunicaciones; en cada nivel o capa el modelo TCP/IP está compuesto por dispositivos y protocolos que establecen comunicaciones a nivel de capas superior ores e inferiores. Se ha establecido que a nivel de TCP/IP soporta los siguientes tipos de interfaces de red:

- **Ethernet** Versión 2 estándar (en), utilizada en enlaces LAN.

- **IEEE 802.3 (et)**, aplicadas en enlace LAN
- **Red en anillo (tr)**, aplicada en enlace LAN.
- **SLIP** (Serial Line Internet Protocol), es para utilizarse con conexiones serie.
- **Bucle de retorno (lo)**, la utiliza un sistema principal para devolverse mensajes a sí mismo.
- **FDDI**
- **Óptica serie (so),** la interfaz óptica serie es para utilizarse con redes ópticas.
- **PPP (Point-to-Point Protocol - Protocolo de punto a punto)**, se utiliza normalmente cuando se conecta a otro sistema o red a través de un módem
- **Dirección IP virtual (vi).** La interfaz de Dirección IP virtual (también denominada interfaz virtual) no está asociada con ningún adaptador de red determinado. Se pueden configurar varias instancias de una interfaz virtual en un sistema principal. Cuando se configuran interfaces virtuales, la dirección de la primera interfaz virtual se convierte en la dirección de origen a menos que una aplicación haya elegido una interfaz diferente. Los procesos que utilizan una dirección IP virtual como dirección de origen pueden enviar paquetes a través de cualquier interfaz de red que proporcione la mejor ruta para dicho destino. Los paquetes de entrada destinados a una dirección IP virtual se entregan al proceso independientemente de la interfaz a través de la cual llegan

Topologías de red

Una topología de red es la estructura de equipos o dispositivos demás componentes en una red. La topología se la establecido a nivel física y lógica.

La **topología física** describe cómo están conectados los componentes físicos de una red, es la conexión física de circuitos.

La **topología lógica** describe el modo en que los datos de la red fluyen a través de componentes físicos, la proporciona el software y es una conexión lógica.

Se detallan las topologías aplicada a nivel y lógico y físico:

Topología punto a punto

Una topología punto a punto conecta dos nodos directamente entre sí. El nodo en un extremo coloca las tramas en los medios y el nodo en el otro extremo las saca de los medios del circuito punto a punto. En redes punto a punto, si los datos sólo pueden fluir en una dirección a la vez, está operando como un enlace half-duplex. Si los datos pueden fluir con éxito a través del enlace desde cada nodo simultáneamente, es un enlace dúplex.

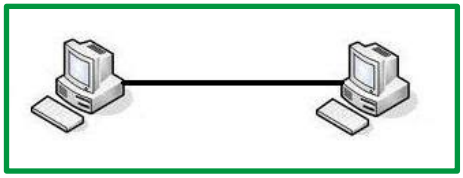


Figura 26: Representación gráfica de topología punto a punto

Topología de bus:

En la topología de bus todos los nodos (computadoras) están conectados a un circuito común (bus). La información que se envía de una computadora a otra viaja directamente o indirectamente, si existe un controlador que enruta los datos al destino correcto. La información viaja por el cable en ambos sentidos a una velocidad aproximada de 10/100/1000 Mbps y tiene en sus dos extremos una resistencia (terminador). Se pueden conectar una gran cantidad de computadoras al bus, si un computador falla, la comunicación se mantiene, no sucede lo mismo si el bus es el que falla. El tipo de cableado que se usa puede ser coaxial, par trenzado o fibra óptica. En una topología de bus, cada computadora está conectada a un segmento común de cable de red. El segmento de red se coloca como un bus lineal, es decir un cable largo que va de un extremo a otro de la red, y al cual se conecta cada nodo de ésta. El cable puede ir por el piso, las paredes, el techo o por varios lugares, siempre y cuando sea un segmento continuo.

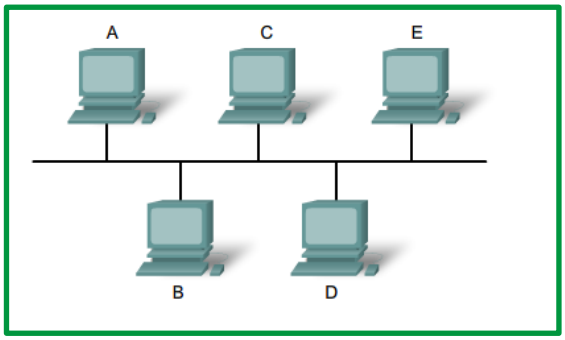


Figura 27: Representación gráfica de topología de bus

Características:

- Es frecuente en las redes de área local.
- Todos los dispositivos de red reciben el paquete de datos.

Ventajas	Desventajas
Simple y fácil de instalar.	Si el canal de comunicaciones falla, toda la red deja de funcionar.
Se usa para redes pequeñas y temporales.	El número de equipos presentes en un bus afecta el rendimiento de la red.
Facilidad para agregar dispositivos a la red.	Es conocida como pasiva porque las computadoras no regeneran la señal, lo que provoca que esta se pierda a través de la distancia del cable.

Topología de estrella:

Reduce la posibilidad de fallo de red conectando todos los nodos a un nodo central. Cuando se aplica a una red basada en la topología estrella este concentrador central reenvía todas las transmisiones recibidas de cualquier nodo periférico a todos los nodos periféricos de la red, algunas veces incluso al nodo que lo envió. Todos los nodos periféricos se pueden comunicar con los demás transmitiendo o recibiendo del nodo central solamente. Un fallo en la línea de conexión de cualquier nodo con el nodo central provocaría el aislamiento de ese nodo respecto a los demás, pero el resto de sistemas permanecería intacto. El tipo de concentrador hub se utiliza en esta topología, aunque ya es muy obsoleto; se suele usar comúnmente un switch.

Figura 28: Representación gráfica de topología estrella

Características:

- Es la más empleada en los sistemas de comunicación de datos.
- Todas las computadoras reciben el mensaje, pero sólo la computadora con la dirección igual a la dirección del mensaje puede leerlo.
- El nodo central es el responsable de encaminar el tráfico hacia el resto de los componentes; se encarga además de localizar las averías.

Ventajas	Desventajas
Si una computadora se desconecta o si se le rompe el cable sólo esa computadora es afectada.	Es costosa ya que requiere más cableado que otras topologías.
Es fácil de reconfigurar; añadir o remover una computadora es tan simple como conectar o desconectar el cable.	Si el hub se cae, la red no tiene comunicación.

Topología anillo:

Una red en anillo es una topología de red en la que cada estación tiene una única conexión de entrada y otra de salida. Cada estación tiene un receptor y un transmisor que hace la función de traductor, pasando la señal a la siguiente estación. En este tipo de red la comunicación se da por el paso de un token o testigo, que se puede conceptualizar como un cartero que pasa recogiendo y entregando paquetes de información, de esta manera se evitan eventuales pérdidas de información debidas a colisiones. En un anillo doble (Token Ring), dos anillos permiten que los datos se envíen en ambas direcciones (Token passing). Esta configuración crea redundancia (tolerancia a fallos). Evita las colisiones.

En esta topología, los equipos están conectados con un cable de forma circular. No hay extremos con terminaciones. Las señales viajan alrededor del bucle en una dirección y pasan a través de cada equipo que actúa como repetidor para amplificar la señal y enviarla al siguiente equipo.

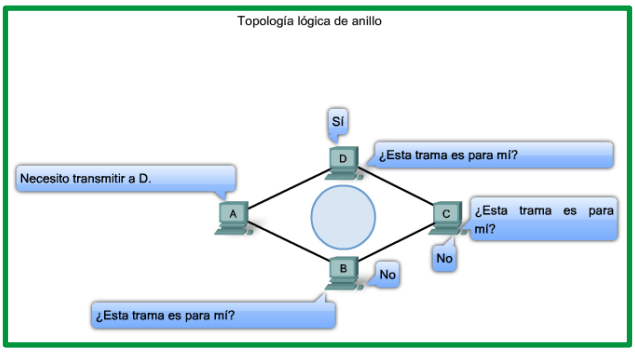


Figura 29: Representación gráfica de topología de anillo

Características:

- Todos los componentes del anillo están unidos por un mismo canal.
- En una topología en anillo cada equipo actúa como repetidor, regenerando la señal y enviándola al siguiente equipo.

Ventajas	Desventajas
La organización en anillo resulta atractiva porque con ella son bastante raros los embotellamientos.	Si falla el canal entre dos nodos, toda la red se interrumpe.
Mínimo costo de instalación, pues para crearla basta con que los equipos cuenten con tarjetas de red y que exista un cable coaxial que una un punto con otro.	Posee una mayor lentitud en la transmisión de la señal debido a que la información es repartida por todo el anillo.
Utilizan menos cable que la topología estrella.	La topología de anillo utiliza más cable que la de bus.

Una variante de la topología de anillo es la aplicación de doble anillo, establecida básicamente para redundancia de enlace.

Topología malla:

Cada equipo está conectado a cada uno del resto de los equipos por un cable distinto. Gracias a los múltiples caminos que ofrece a través de los distintos dispositivos, es posible orientar el tráfico por trayectorias alternativas en caso de que algún nodo esté averiado u ocupado. Este tipo de tecnología requiere mucho cable (cuando se utiliza el cable como medio, pero puede ser inalámbrico también). Pero debido a la redundancia, la red puede seguir operando si una conexión se rompe.

Una red con topología en malla ofrece una redundancia y fiabilidad superiores. Aunque la facilidad de solución de problemas y el aumento de la confiabilidad son ventajas muy interesantes, estas redes resultan caras de instalar.

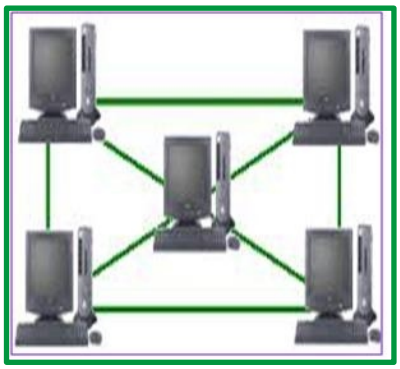


Figura 30: Representación gráfica de topología malla

Características:

- Cada nodo está conectado a todos los nodos.
- Es posible llevar los mensajes de un nodo a otro por distintos caminos.

Ventajas	Desventajas
Los enlaces dedicados garantizan que cada conexión sólo debe transportar la carga de datos propia de los dispositivos conectados.	Debido a las rutas redundantes requieren más cable del que se necesita en otras topologías.
Una topología en malla es robusta. Si un enlace falla, no inhabilita todo el sistema.	Requiere n-1 puertos de comunicación.
Privacidad y seguridad. Cuando un mensaje viaja a través de una línea dedicada, solamente lo ve el receptor adecuado.	El mantenimiento resulta costoso a largo plazo.

Topología árbol o topología jerárquica:

Una topología de árbol o topología jerárquica es aquella que combina características de la topología estrella con la de bus, se podría decir que es una combinación de ambas.

Figura 31: Representación gráfica de topología de árbol

Trabaja de la misma manera que la de bus y estrella por el modo de actuar del nodo ya que el nodo de interconexión trabaja en modo difusión, pues la información se propaga hacia todas las estaciones, solo que en esta topología las ramificaciones se extienden a partir de un punto raíz

como la de estrella, a tantas ramificaciones como sean posibles, según las características del árbol.

Características:

- Gran parte de los dispositivos se conectan a un concentrador secundario que, a su vez, se conecta al concentrador central.

Ventajas	Desventajas
Soportado por multitud de vendedores de software y de hardware.	Si se viene abajo el segmento principal, todo el segmento se viene abajo con él.
Da lugar a la creación de nuevas redes y/o subredes tanto internas como externas, lo que facilita el crecimiento de la red.	Las redes de computadoras se montan con una serie de componentes de uso común y que en mayor o menor medida aparece siempre en cualquier instalación.
Cableado punto a punto para segmentos individuales.	La medida de cada segmento viene determinada por el tipo de cable utilizado. Además de que su configuración es más difícil.

Topología Hibrida o Mixta:

Las redes pueden utilizar diversas tipologías para conectarse, como por ejemplo en estrella. La topología híbrida es una de las más frecuentes y se deriva de la unión de varios tipos de topologías de red, de aquí el nombre de híbridas. Ejemplos de topologías híbridas serían: en árbol, estrella-estrella, bus-estrella, etc.

Su implementación se debe a la complejidad de la solución de red, o bien al aumento en el número de dispositivos, lo que hace necesario establecer una topología de este tipo. Las topologías híbridas tienen un costo muy elevado debido a su administración y mantenimiento, ya que cuentan con segmentos de diferentes tipos, lo que obliga a invertir en equipo adicional para lograr la conectividad deseada.

Métricas de desempeño de red y tráfico

Se obtienen un mayor desempeño en las redes con el establecimiento y análisis de todos los aspectos que intervienen en la comunicación, estas mediciones se basan en los valores determinados por las métricas.

A continuación de establecen las métricas más comunes relativas al tráfico de red:

- Bits por segundo
- Paquetes por segundo
- Paquetes unicast vs. paquetes no-unicast
- Errores
- Paquetes descartados
- Flujo por segundo
- Tiempo de ida y vuelta (RTT)
- Dispersión del retardo (parpadeo o “jitter”)

Las métricas se enfocan en tres aspectos:

- Red
- Sistemas
- Servicios.

Métricas de rendimiento de red.

- **Capacidad del canal**:
  - **Nominal**: Máxima cantidad de datos transmitidos por unidad de tiempo. Ejemplo: bits por segundo, paquetes por minuto.

    Depende de:

    - ✓ Ancho de banda del medio físico
    - ✓ Cable
    - ✓ Ondas electromagnéticas
    - ✓ Fibra óptica
    - ✓ Líneas de cobre
    - ✓ Capacidad de procesamiento de elementos transmisores
    - ✓ Eficiencia de los algoritmos de acceso al medio
    - ✓ Mecanismos de codificación de canal
    - ✓ Mecanismos de compresión de datos
  - **Efectiva**: Fracción de la capacidad nominal.

    CapacidadEfectiva = **N** x **CapacidadNominal** (Siempre N < 1)

    La capacidad efectiva se ve afectada por varios factores:

    - ✓ Carga adicional de procesamiento en las varias capas OSI
    - ✓ Limitaciones de procesamiento en dispositivos
    - ✓ Memoria, CPU, otros
    - ✓ Eficiencia del protocolo de transmisión
    - ✓ Control de flujo.
    - ✓ Enrutamiento
- **Utilización del canal**: Fracción de la capacidad nominal de un canal que está siendo realmente utilizada. El sistema de medición 95 % percentil (95th percentile, en inglés) se establece para medir el consumo de ancho de banda, es el método más eficiente para medir y facturar el ancho de banda de un servicio.

  Se factura al cliente: N x Costo por unidad (ejemplo: 40 Mbit/s x $30.00 Mbits = $120.00 al mes).

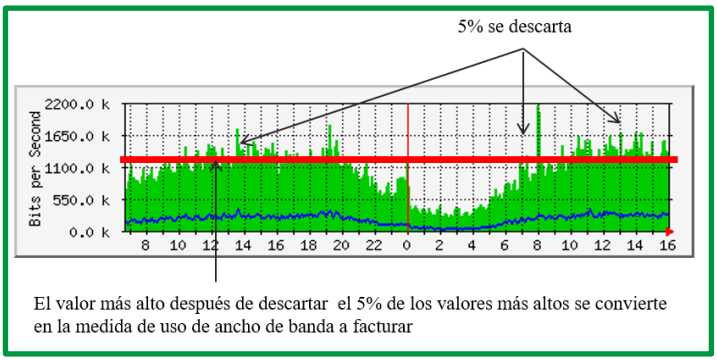


Figura 32: Facturación de uso de canal con el sistema de medición 95 % percentil

- **Retardo y jitter**
  - **Retardo**: es el tiempo transcurrido en transmitir un paquete de fuente a destino final producido por una aplicación, entregado al sistema operativo, pasado a la tarjeta de red, codificado, transmitido por el medio físico, recibido por un equipo intermedio (switch, router), analizado, retransmitido en otro medio...etc., etc. La medición más común es de ida y vuelta (RTT). El utilitario ping se usa para medir esta variable.

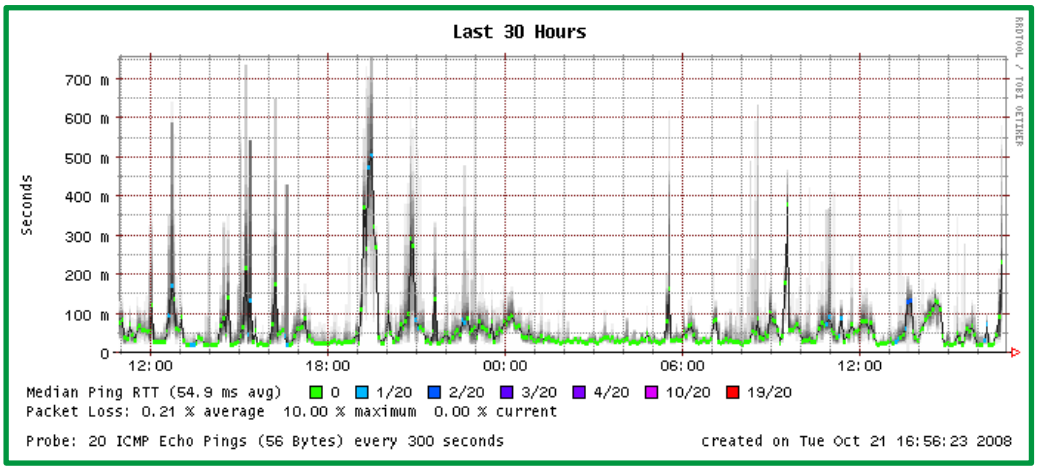


Figura 33: Captura de trafico de red para análisis de retardo.

Componentes del retardo extremo a extremo:

- ✓ **Retardo de Procesamiento**: Tiempo requerido en analizar el encabezado y decidir a dónde enviar el paquete.
- ✓ **Retardo de Colas**: Tiempo en que el paquete espera en un búfer hasta ser transmitido.
- ✓ **Retardo de Transmisión**: Tiempo requerido para pasar todos los bits de un paquete a través del medio de transmisión:

  d = L/R

  R= tasa de bits, (o velocidad de transferencia de datos)

  L=Longitud del paquete,

  d = retardo
- ✓ **Retardo de Propagación**: es el tiempo transcurrido en su propagación hasta el final del medio una vez que el bit de dato entra al medio físico. La

velocidad de propagación del enlace depende más que nada de la distancia medio físico. Para d = distancia, s = velocidad de propagación => Dp = d/s

  - **Jitter:** Son las variaciones de retardo que se presentan entre paquetes. Por ejemplo, un paquete llega con un retardo de 10 ms al destino y el segundo paquete, con un retardo de 30 ms; entonces el jitter es de 20 ms entre paquetes.
- **Pérdida de paquetes y errores:** Ocurren por el hecho de que las colas (búfers) no son infinitas. Para contrarrestar este problema se aplican técnicas de control de flujo para evitar congestiones y tráfico en la red.

*Rendimiento de sistemas***.**

Estas métricas se basan en consideran lo siguiente:

- Disponibilidad (UP, DOWN, UNREACHABLE)
- Memoria, utilización y carga de CPU
- Utilización de dispositivos de entrada/salida

Rendimiento de servicios. Se consideran dos factores:

- Disponibilidad
- Tiempo de acceso y carga

Métricas consideradas en nivel de protocolos de enrutamiento

Los desempeños de las redes están definidas a nivel varios aspectos, a nivel de enrutamiento los diferentes protocolos de enrutamiento pueden usar diferentes métricas. La métrica utilizada por un protocolo de enrutamiento no es comparable con la métrica utilizada por otro protocolo de enrutamiento. Dos protocolos de enrutamiento diferentes pueden elegir diferentes rutas hacia el mismo destino debido al uso de diferentes métricas.

Se puede ejemplificar indicando que RIP elegirá la ruta con la menor cantidad de saltos, mientras que OSPF elegirá la ruta con el ancho de banda superior.

Para seleccionar el mejor camino, el protocolo de enrutamiento debe poder evaluar y diferenciar entre las rutas disponibles. Para tal fin, se usa una métrica. Una métrica es un valor utilizado por los protocolos de enrutamiento para asignar costos a fin de alcanzar las redes remotas. La métrica se utiliza para determinar qué ruta es más preferible cuando existen múltiples rutas hacia la misma red remota.

Cada protocolo de enrutamiento usa su propia métrica. Por ejemplo, RIP usa el conteo de saltos, EIGRP usa una combinación de ancho de banda y retardo, y la implementación de OSPF de Cisco usa el ancho de banda. El conteo de saltos es la métrica más sencilla para hacer previsiones. El conteo de saltos se refiere a la cantidad de routers que debe atravesar un paquete para llegar a la red de destino. Para R3 en la figura, la red 172.16.3.0 se encuentra a dos saltos o dos routers de distancia.

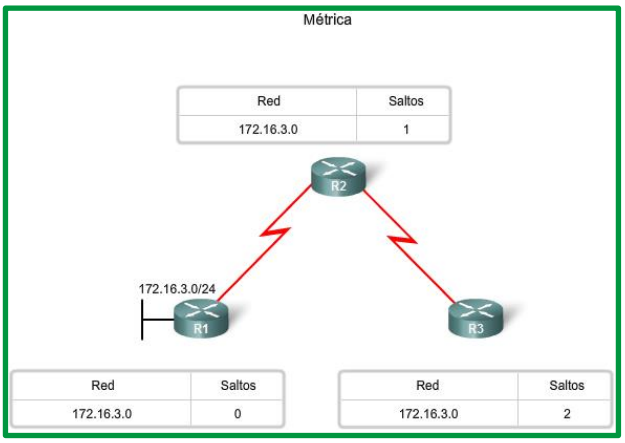


Figura 34: Métricas que se establece por el número de saltos en protocolo de enrutamiento

Las métricas utilizadas en los protocolos de enrutamiento IP incluyen:

- **Conteo de saltos**: una métrica simple que cuenta la cantidad de routers que un paquete tiene que atravesar.
- **Ancho de banda**: influye en la selección de rutas al preferir la ruta con el ancho de banda más alto.
- **Carga**: considera la utilización de tráfico de un enlace determinado.
- **Retardo**: considera el tiempo que tarda un paquete en atravesar una ruta.
- **Confiabilidad**: evalúa la probabilidad de una falla de enlace calculada a partir del conteo de errores de la interfaz o las fallas de enlace previas.
- **Costo**: un valor determinado ya sea por el Cisco IOS o por el administrador de red para indicar la preferencia de una ruta. El costo puede representar una métrica, una combinación de las mismas o una política.

A continuación, se establecen las métricas que se consideran en algunos protocolos de enrutamiento:

- **RIP**: conteo de saltos; el mejor camino se elige teniendo en cuenta la ruta con la menor cantidad de saltos.
- **IGRP** y **EIGRP**: ancho de banda, retardo, confiabilidad y carga; el mejor camino se elige según la ruta con el valor de métrica compuesto más bajo calculado a partir de estos múltiples parámetros. De manera predeterminada, sólo se usan el ancho de banda y el retardo.
- **IS-IS** y **OSPF**: costo; el mejor camino se elige según la ruta con el costo más bajo. La implementación de OSPF de Cisco usa el ancho de banda. El IS-IS se analiza en CCNP.

Los protocolos de enrutamiento determinan el mejor camino en base a la ruta con la métrica más baja.

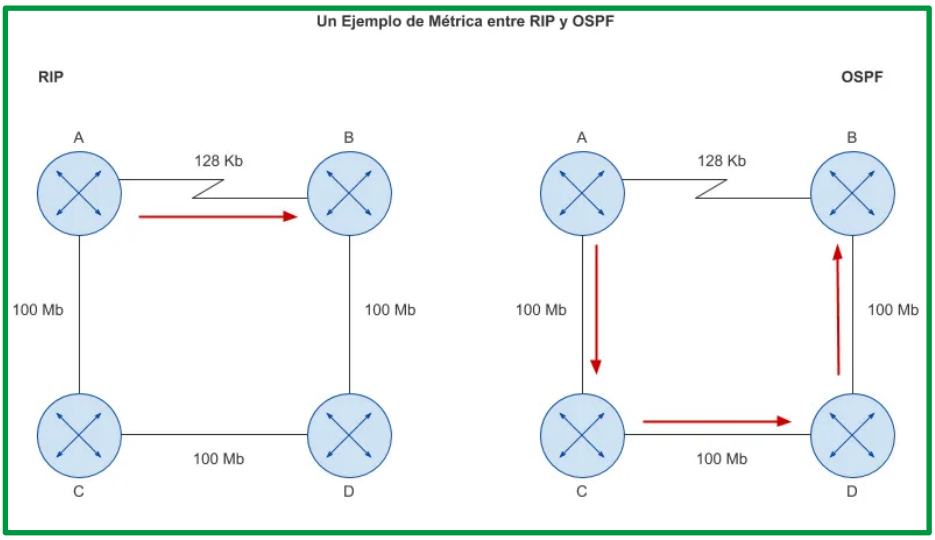


Figura 35: Comparación de métricas utilizada en el protocolo RIP y OSPF

Como se observa en la figura 35, el protocolo RIP establece la ruta más corta si analizar el ancho de banda que utilizará (128 kb), mientras el protocolo OSPF establece como métrica el ancho de banda de 100 Mbps pese a la ruta es más larga (3 saltos) pero con un mejor ancho de banda.

Trafico convergente.

¿Qué es una red convergente?

La convergencia es el proceso de combinación de las comunicaciones de datos, voz y video en una red de datos. Las redes convergentes inicialmente fueron factibles en grandes organizaciones empresariales, sus requisitos en infraestructura de la red y a la compleja administración necesaria que funcionen en forma continua demandaban inversiones tecnológicas.

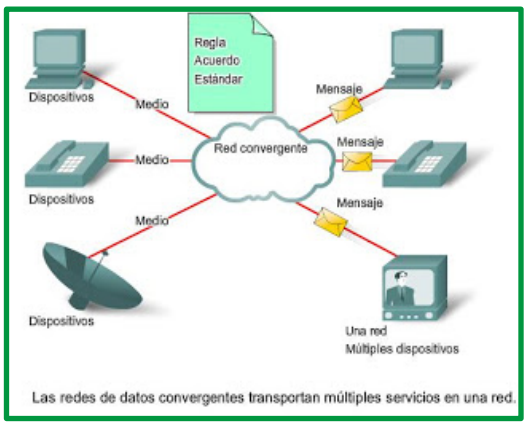


Figura 36: Datos en una red convergente

En el diseño de una red convergente es necesario considerar la velocidad de transmisión (Vtx) del canal. Es indispensable que se disponga de una Vtx suficiente para la transmisión de voz, datos, audio y video, caso contrario surgirán problemas de retardos, que en aplicaciones como la telefonía y la videoconferencia son factores adversos e influyentes para la degradación de la comunicación.

Los dos principales tipos de tráfico en una red convergente:

- Transmisión de datos sobre tecnología IP
- Transmisión de voz y video sobre tecnología IP

Actualmente, la nube convergente es la apuesta de las empresas de networking, es el siguiente paso que se ejecuta una vez posesionado el cloud computing.

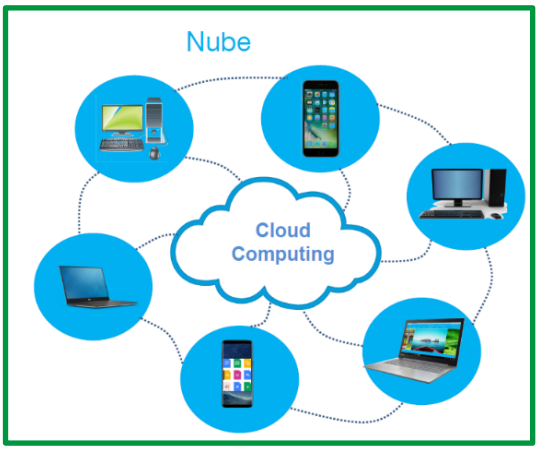


Figura 37: Nube

Hardware de redes.

Está formado por los componentes materiales que conectan los ordenadores. Los dos principales componentes están definidos por el ***medio de transmisión*** que transportan las señales de los ordenadores y el ***adaptador de red***, que permite acceder al medio material que conecta a los ordenadores, recibir paquetes desde el software de red y transmitir instrucciones y peticiones a otras computadoras. La información se transfiere en forma de dígitos binarios, o bits (unos y ceros), que pueden ser procesados por los circuitos electrónicos de los ordenadores.

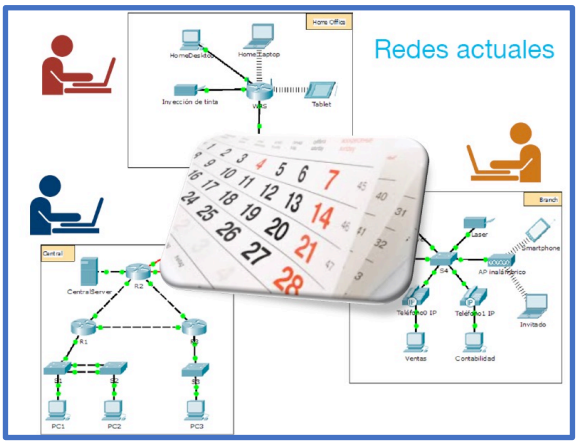


Figura 38: redes actuales

Software de redes.

El software de red consiste en programas informáticos que establecen protocolos o normas, para que los equipos se comuniquen entre sí. Estos protocolos se aplican enviando y recibiendo grupos de datos formateados denominados paquetes. Los protocolos indican cómo efectuar conexiones lógicas entre las aplicaciones de la red, dirigir el movimiento de paquetes a través de la red física y minimizar las posibilidades de colisión entre paquetes enviados simultáneamente

además los programas de red hacen posible la comunicación entre las computadoras, permiten compartir recursos (software y hardware) y ayudan a controlar la seguridad de dichos recursos.

En el presente apartado es necesario detallar el paradigma de las redes definidas por software, conocida comúnmente por sus siglas en inglés como SND.

Según cisco, Las redes definidas por software (SDN) están diseñadas para flexibilizar y agilizar la red. Las SDN le permiten diseñar, desarrollar y administrar redes mediante la separación de los planos de control y reenvío. Como resultado, el plano de control se puede programar directamente, y abstrae la infraestructura subyacente para las aplicaciones y los servicios de red.

La inteligencia de red se centraliza de manera lógica a través de controladores SDN programables. Implementados en el software, estos controladores mantienen una vista coherente del dominio de red. Para los motores de aplicaciones y políticas, las SDN son como un switch lógico.

Las redes definidas por software (SDN) ofrecen una red centralizada y programable que consiste en un controlador SDN, API descendentes y API ascendentes.

- Los controladores SDN son los cerebros de la red, ya que ofrecen una vista centralizada de toda la red.
- Las API descendentes transmiten información a los switches y routers de la red.
- Las API ascendentes se comunican con las aplicaciones y los servicios de implementación.

La virtualización de funciones de red (NFV) utiliza tecnología de hipervisor y computación en la nube para la organización y la automatización de la red. La NFV funciona mejor en el contexto de los servicios de red (OSI nivel 4 y superior) que requieren una alta potencia de cálculo con un rendimiento del ancho de banda de bajo a medio.

Las SDN combinan la administración de servicios de redes y de aplicaciones en plataformas de organización centralizadas y extensibles. Las SDN son óptimas para el reenvío de red de alto rendimiento (OSI niveles 0 a 3) donde las cargas de trabajo con uso intensivo del ancho de banda necesitan una administración de tráfico significativa. Se establece a continuación a la arquitectura SDN:

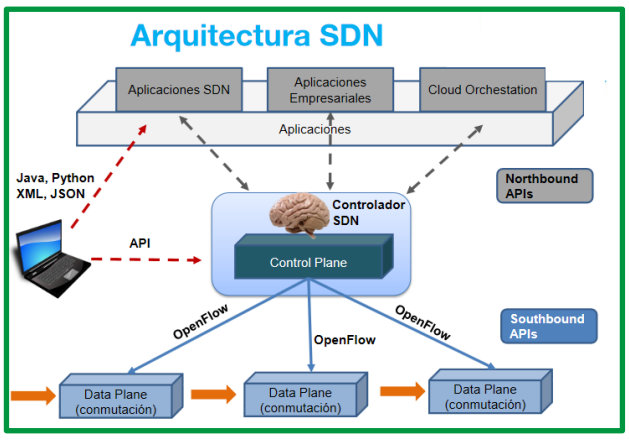


Figura 39: Arquitectura SDN

Tema 2: Clasificación de las redes

Las redes de comunicaciones se clasifican por su alcance geográfico en:

- Redes LAN
- Redes WAN
- Redes MAN

Redes LAN

LAN (Local Area Network), es una red que cubre una única área geográfica que proporciona servicios, aplicaciones y recursos compartidos a sus usuarios dentro de una estructura organizacional común, como una empresa, un campus o una región.

Las redes LAN normalmente es administrada por una organización única. El control administrativo que rige las políticas de seguridad y control de acceso está implementado en el nivel de red.

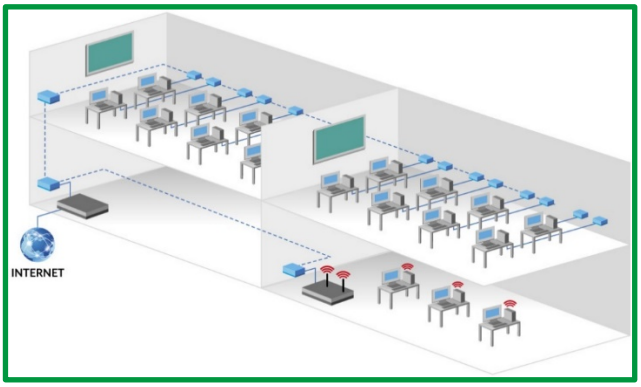


Figura 40: Redes LAN

Redes WAN

WAN (Wide Area Network), son redes que se extienden sobre un área geográfica extensa, conectan las LAN en ubicaciones separadas geográficamente. Los hosts de estas LAN acceden a la subred de la WAN por medio de un dispositivo de enrutamiento. Las velocidades de transmisión varían según la tecnología de conexión utilizada.

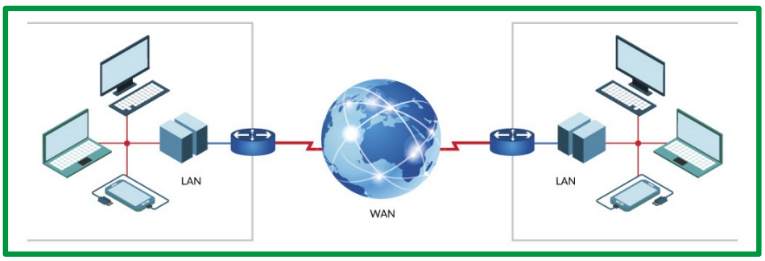


Figura 41: Redes WAN

Redes MAN

MAN (Metropolitan Area Network), la red de área metropolitana es una red de telecomunicaciones de banda ancha que comunica varias redes LAN en una zona geográficamente cercana. Por lo general, se trata de cada una de las sedes de una empresa u organización que se agrupan en una MAN por medio de líneas arrendadas.

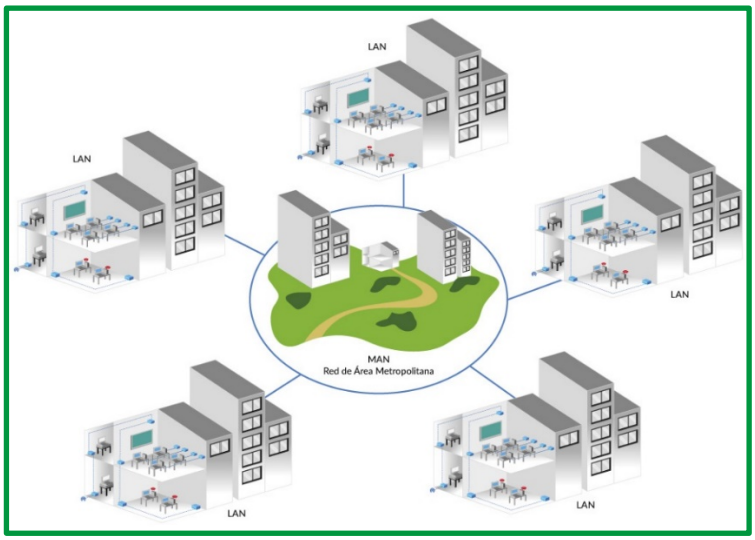


Figura 42: Redes MAN

Otros tipos de redes

Personal Area Networks (PAN), es la red de área personal que se utiliza para conectar dispositivos finales entre sí a otras redes de mayor tamaño.

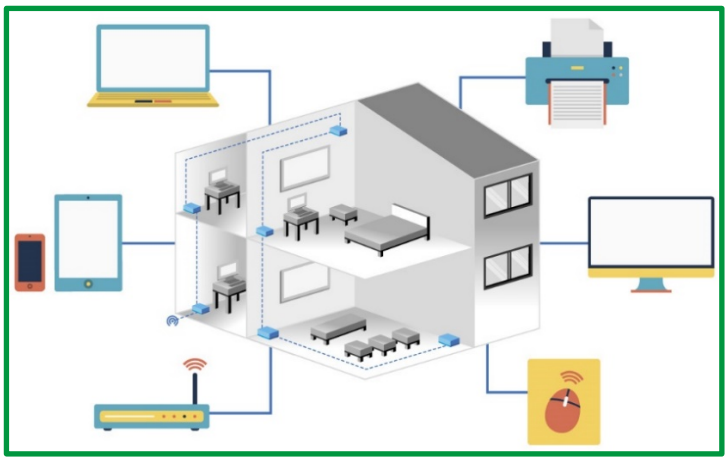


Figura 43: Redes PAN

Global Area Networks (GAN), es la red de área global o conocida como Internetwork que consiste en una malla global de redes interconectadas (internetworks) cubre estas necesidades de comunicación humanas.

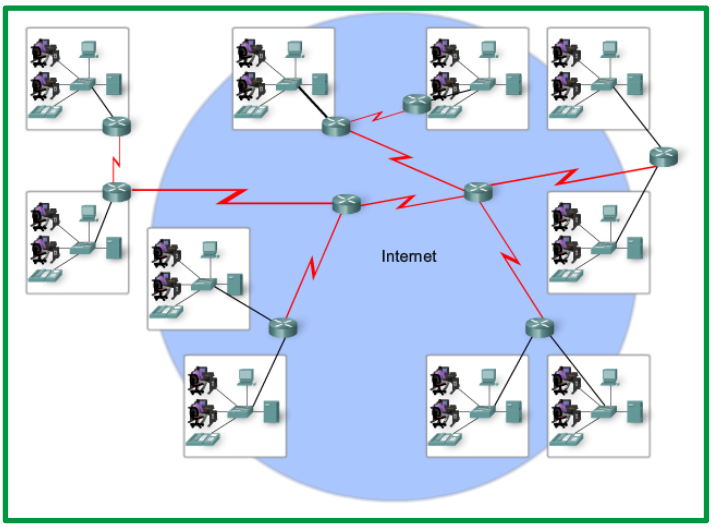


Figura 44: Internet

Red SAN (Storage Area Network), una SAN es una red compuesta por unidades de almacenamiento que se conectan a las redes de área local de las compañías u organizaciones. Su aplicación está orientada a dar servicios a empresas, para resguardar importantes volúmenes. El crecimiento exponencial de la información almacenada en los centros de procesamiento de las empresas, cuestión generada por la informatización avanzada y la evolución de las comunicaciones, ha llevado a la industria a crear soluciones más eficientes para administrar el almacenamiento de los datos.

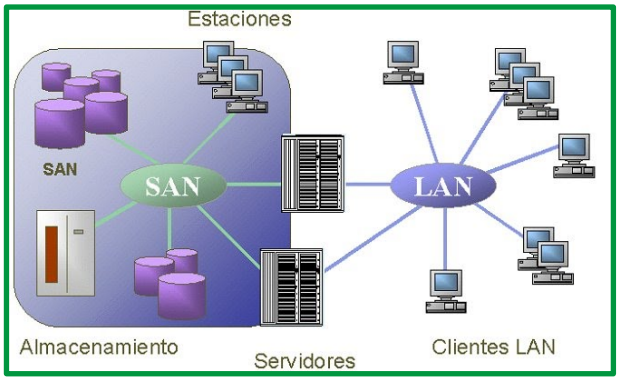


Figura 45: Redes SAN

Backbone Network. Este tipo de red es de amplitud geográfica que cubre la conexión de un país y hasta un continente.

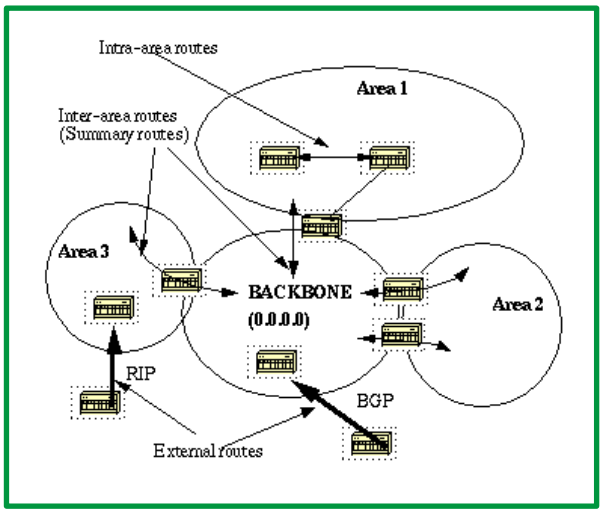


Figura 46: Backbone

Redes de comunicación lógicas, Virtual Private Networks (VPN), es una red de comunicación virtual que utiliza la infraestructura de una red física para asociar sistemas informáticos de manera lógica. las Virtual Private Networks o redes privadas virtuales suelen cifrarse para garantizar la confidencialidad de los datos. Las VPN se emplean para conectar redes LAN en Internet o para hacer posible el acceso remoto a una red o a un único ordenador a través de la conexión pública.

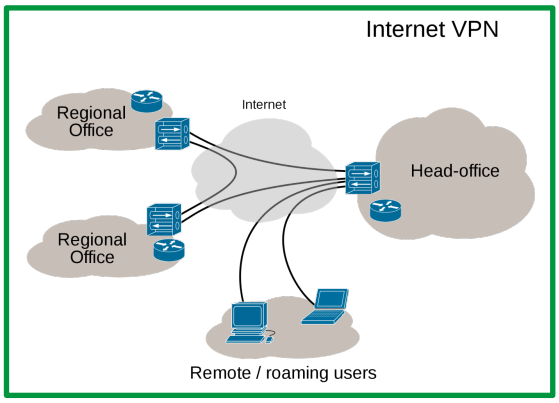


Figura 43: Redes VPN

Es importante indicar que dentro de los tipos de redes también se encuentran las tecnologías inalámbricas, entre esta WPAN, WLAN, WWAN, WLAN que se diferencian por la utilización de medios no guiados.

Tema 3: Arquitectura de red (OSI y TCP/IP)

En la década durante la década de los 70, un grupo de ingenieros e investigadores, había desarrollado una arquitectura basada en protocolos de aplicación en la red ARPANET. Se trataba de la arquitectura que hoy se conoce como TCP/IP, siendo actualmente la más difundida para la comunicación en redes de datos.

En la década de los 80 se produce un crecimiento caótico de las redes por el nacimiento de nuevas tecnologías, la ISO para solventar estos inconvenientes conformó un comité para que

generara un modelo estándar que rigiera las comunicaciones, surge así el modelo de referencia OSI.

En un entorno de comunicación en red, los sistemas no utilizan un único protocolo, sino un conjunto denominado pila o arquitectura de protocolos, que actúan de manera cooperativa, debiendo ser capaces de comunicarse entre sí. El conjunto de protocolos que facilitan la comunicación entre dispositivos se le denomina arquitectura de la red.

Cuando se diseña una red es necesario resolver múltiples problemas: ¿Hay que corregir errores? ¿Qué medio de transmisión vamos a utilizar? ¿cómo distinguimos el ordenador al que hay que enviar la información? ¿hay que codificar la información?

Como respuesta a esta complejidad surgen las arquitecturas por capas que simplifican el diseño y la implementación de las soluciones. En un intento de estandarizar y definir las capas necesarias se crea el modelo de referencia OSI.

Hay gran cantidad de protocolos que han aportado soluciones diferentes a los problemas de red: Netbeui, AppelTalk, TCP/IP, etc. Entre ellos destaca hoy en día TCP/IP que se ha impuesto como estándar de facto en todo tipo de redes. Hoy en día incluso los protocolos propietarios se implementan como interfaces de TCP/IP.

Existen dos tipos básicos de modelos de networking: modelos de protocolo TCP/IP y modelos de referencia OSI.

El modelo TCP/IP es un modelo de protocolo porque describe las funciones que se producen en cada capa de los protocolos dentro del conjunto TCP/IP.

El modelo de interconexión de sistema abierto (OSI) es el modelo de referencia de internetwork más ampliamente conocido. Se utiliza para el diseño de redes de datos, especificaciones de funcionamiento y resolución de problemas. Un modelo de referencia no está pensado para ser una especificación de implementación ni para proporcionar un nivel de detalle suficiente para definir de forma precisa los servicios de la arquitectura de red. El propósito principal de un modelo de referencia es asistir en la comprensión más clara de las funciones y los procesos involucrados.

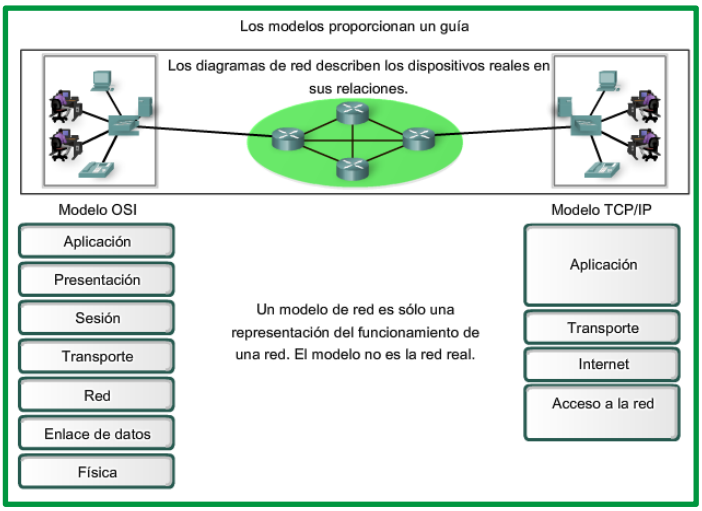


Figura 48: Modelo de referencia OSI y Modelo TCP/IP

Modelo basado en niveles

Para proceso de estudio y comprensión, a nivel de redes de datos se aplican dos modelos en capas que muestra el funcionamiento de los protocolos que se produce dentro de cada capa, como así también la interacción de las capas un nivel abajo y un nivel arriba sobre la capa estudiada.

Existen beneficios al utilizar un modelo en capas, para describir los protocolos de red y el funcionamiento. El uso de un modelo en capas:

- Asiste en el diseño del protocolo, porque los protocolos que operan en una capa específica poseen información definida que van a poner en práctica y una interfaz definida según las capas por encima y por debajo.
- Fomenta la competencia, ya que los productos de distintos proveedores pueden trabajar en conjunto.
- Evita que los cambios en la tecnología o en las capacidades de una capa afecten otras capas superiores e inferiores.
- Proporciona un lenguaje común para describir las funciones y capacidades de red.

Modelo de referencia de interconexión de sistemas abiertos (OSI)

El modelo OSI fue diseñado por la Organización Internacional para la Estandarización (ISO, International Organization for Standardization) para proporcionar un marco sobre el cual crear una suite de protocolos de sistemas abiertos. La visión era que este conjunto de protocolos se utilizara para desarrollar una red internacional que no dependiera de sistemas propietarios.

La velocidad a la que fue adoptada el protocolo de internet basada en TCP/IP y la proporción en la que se expandió ocasionaron que el desarrollo y la aceptación de la suite de protocolos OSI quedaran atrás. Aunque pocos de los protocolos desarrollados mediante las especificaciones OSI son de uso masivo en la actualidad, el modelo OSI de siete capas ha realizado aportes importantes para el desarrollo de otros protocolos y productos para los tipos de nuevas redes.

Como modelo de referencia, el modelo OSI proporciona una amplia lista de funciones y servicios que pueden producirse en cada capa. También describe la interacción de cada capa con las capas directamente por encima y por debajo de él. A continuación, se detallan los sietes capas del modelo OSI.

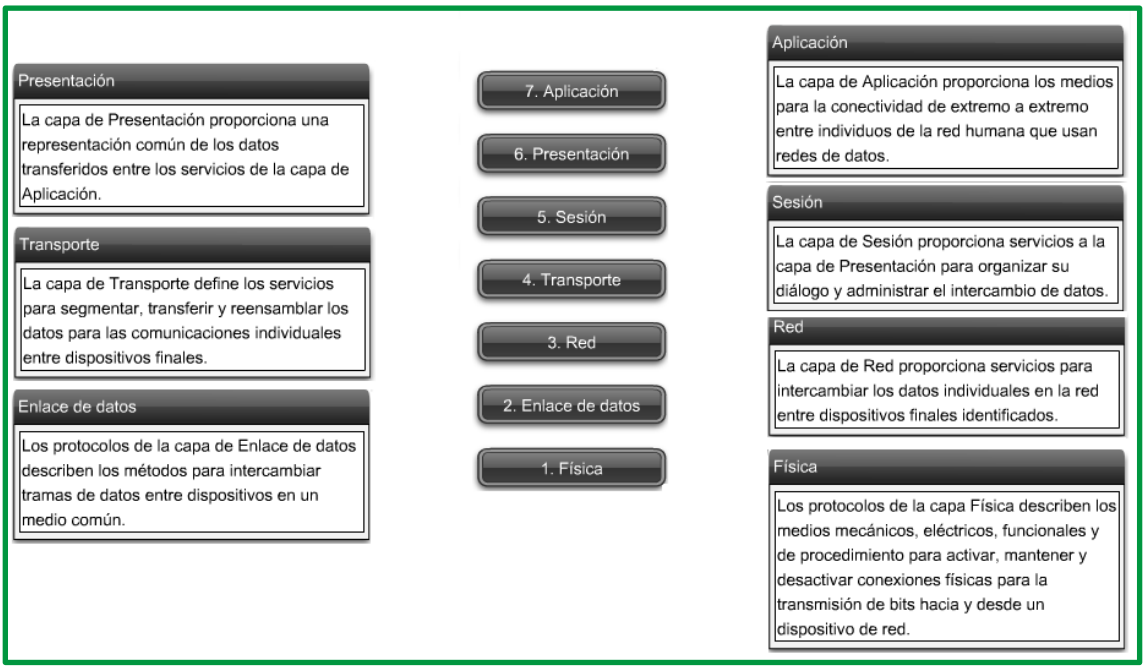


Figura 49: Capas del modelo OSI.

Las diferentes funciones establecidas en la arquitectura OSI se han estructurado en siete niveles. Cada nivel tiene unas funciones perfectamente definidas. Las funciones asignadas a los diferentes niveles se complementan entre sí.

Capa Física:

La función de la capa física de OSI es la de codificar en señales los dígitos binarios que representan las tramas de la capa de Enlace de datos, además de transmitir y recibir estas señales a través de los medios físicos (alambres de cobre, fibra óptica o medio inalámbrico) que conectan los dispositivos de la red.

La capa física de OSI proporciona los medios de transporte para los bits que conforman la trama de la capa de Enlace de datos a través de los medios de red. Esta capa acepta una trama completa desde la capa de Enlace de datos y lo codifica como una secuencia de señales que se transmiten en los medios locales. Un dispositivo final o un dispositivo intermedio recibe los bits codificados que componen una trama.

El envío de tramas a través de medios de transmisión requiere los siguientes elementos de la capa física:

- Medios físicos y conectores asociados.
- Una representación de los bits en los medios.
- Codificación de los datos y de la información de control.
- Sistema de circuitos del receptor y transmisor en los dispositivos de red.

El objetivo de la capa física es crear la señal óptica, eléctrica o de microondas que representa a los bits en cada trama. Luego, estas señales se envían por los medios una a la vez.

Otra función de la capa física es la de recuperar estas señales individuales desde los medios, restaurarlas para sus representaciones de bit y enviar los bits hacia la capa de Enlace de datos como una trama completa.

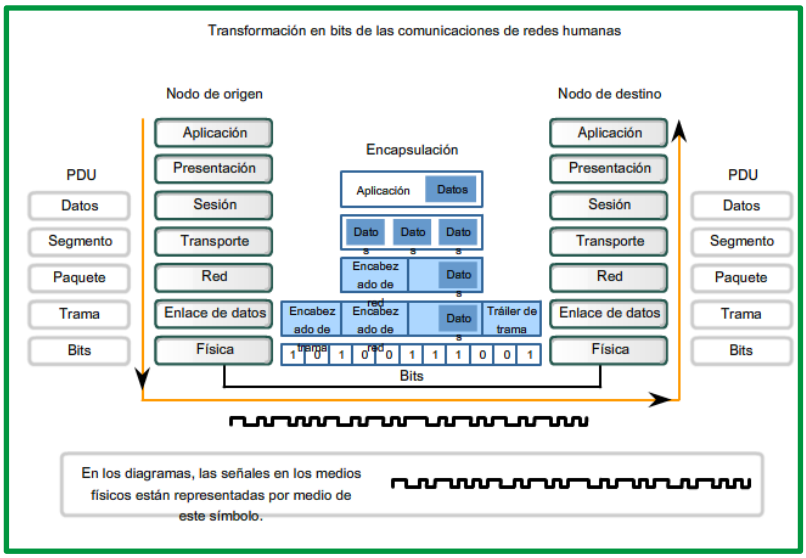


Figura 50: Transformación en bits de las comunicaciones en la capa física

Los medios no transportan la trama como una única entidad. Los medios transportan señales, una por vez, para representar los bits que conforman la trama.

Existen tres tipos básicos de medios de red en los cuales se representan los datos:

- Cable de cobre
- Fibra
- Inalámbrico

La presentación de los bits -es decir, el tipo de señal- depende del tipo de medio. Para los medios de cable de cobre, las señales son patrones de pulsos eléctricos. Para los medios de fibra, las señales son patrones de luz. Para los medios inalámbricos, las señales son patrones de transmisiones de radio.

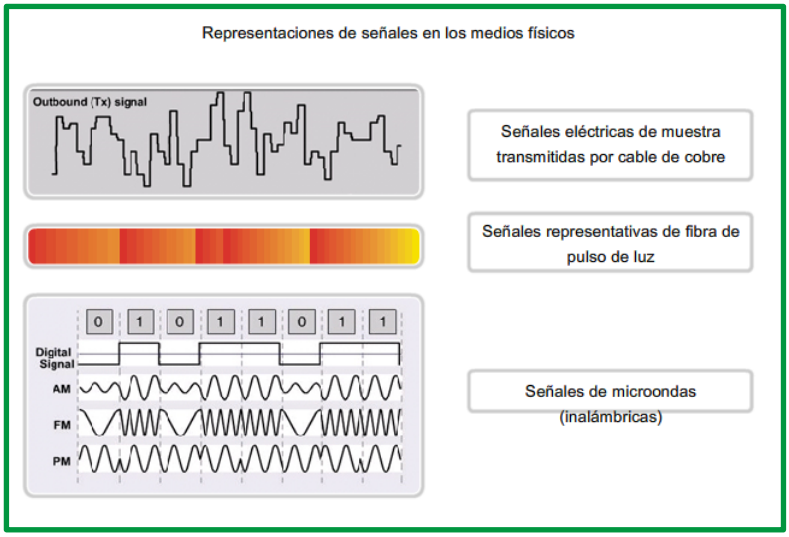


Figura 51: Representaciones de señales en los medios físicos.

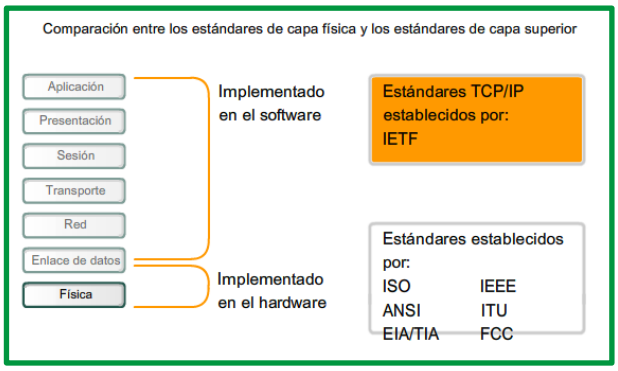


Figura 52: Comparación entre los estándares de capa física y capas superiores

Hardware y tecnologías de la Capa física

Las tecnologías definidas por estas organizaciones incluyen cuatro áreas de estándares de la capa física:

- Propiedades físicas y eléctricas de los medios
- Propiedades mecánicas (materiales, dimensiones, diagrama de pines) de los conectores
- Representación de los bits por medio de las señales (codificación)
- Definición de las señales de la información de control

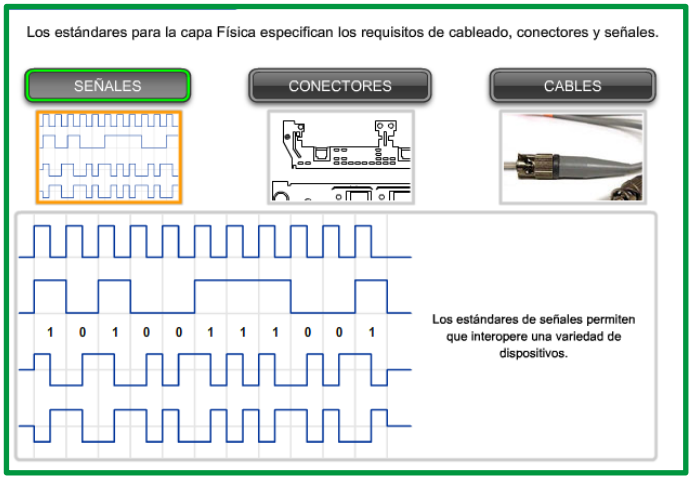


Figura 53: Señales aplicada en la capa Física.

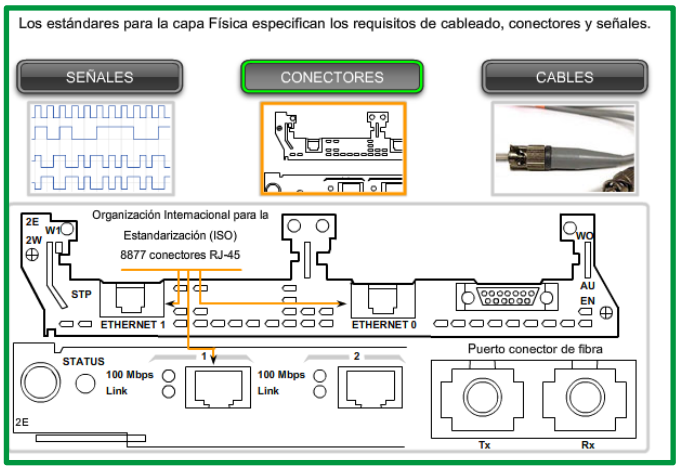


Figura 54: Conectores aplicada en la capa Física.

Figura 55: Cables aplicada en la capa física.

Las tres funciones esenciales de la capa física son:

- Los componentes físicos
- Codificación de datos
- Señalización

Los elementos físicos son los dispositivos electrónicos de hardware, medios y conectores que transmiten y transportan las señales para representar los bits.

Codificación

La codificación es un método utilizado para convertir un stream de bits de datos en un código predefinido. Los códigos son grupos de bits utilizados para ofrecer un patrón predecible que pueda reconocer tanto el emisor como el receptor. La utilización de patrones predecibles permite distinguir los bits de datos de los bits de control y ofrece una mejor detección de errores en los medios.

Además de crear códigos para los datos, los métodos de codificación en la capa física también pueden proporcionar códigos para control, como la identificación del comienzo y el final de una trama. El host que realiza la transmisión transmitirá el patrón específico de bits o un código para identificar el comienzo y el final de la trama.

Señalización

La capa física debe generar las señales inalámbricas, ópticas o eléctricas que representan el "1" y el "0" en los medios. El método de representación de bits se denomina método de señalización. Los estándares de capa física deben definir qué tipo de señal representa un "1" y un "0". Esto puede ser tan sencillo como un cambio en el nivel de una señal eléctrica, un impulso óptico o un método de señalización más complejo.

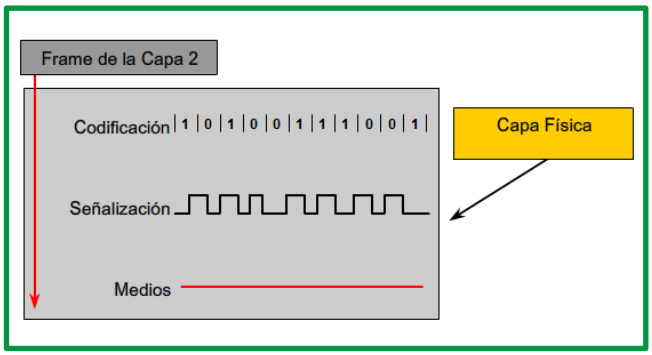


Figura 56: Principios fundamentales de la capa Física.

Capa enlace de datos:

La función de la capa de enlace de datos de OSI es preparar los paquetes de la capa de red para ser transmitidos y controlar el acceso a los medios físicos.

El nivel de enlace de datos se encarga de que los datos se envíen libres de errores a su destino. Se ocupa del tratamiento de los errores que se produzcan en la recepción de las tramas, de eliminar tramas erróneas, solicitar retransmisiones, descartar tramas duplicadas, adecuar el flujo de datos entre emisores rápidos y receptores lentos, etc.

La capa de enlace de datos proporciona un medio para intercambiar datos a través de medios locales comunes. La capa de enlace de datos realiza dos servicios básicos:

- Permite a las capas superiores acceder a los medios usando técnicas, como tramas.
- Controla cómo los datos se ubican en los medios y son recibidos desde los medios usando técnicas como control de acceso a los medios y detección de errores.

Como con cada una de las capas OSI, existen términos específicos para esta capa:

- **Trama**: el PDU de la capa de enlace de datos.
- **Nodo**: la notación de la Capa 2 para dispositivos de red conectados a un medio común.
- **Medios/medio (físico)*:** los medios físicos para la transferencia de información entre dos nodos.
- **Red (física)**:** dos o más nodos conectados a un medio común.

La capa de enlace de datos es responsable del intercambio de tramas entre nodos a través de los medios de una red física.

*Es importante comprender el significado de las palabras medio y medios, se refieren al material que realmente transporta las señales que representan los datos transmitidos. Los medios son el cable de cobre, la fibra óptica físicos o el entorno a través de los cuales la señal viaja.

****Una red física es diferente de una red lógica**. Las redes lógicas se definen en la capa de red mediante la configuración del esquema de direccionamiento jerárquico. Las redes físicas representan la interconexión de dispositivos de medios comunes. Algunas veces, una red física también es llamada segmento de red.

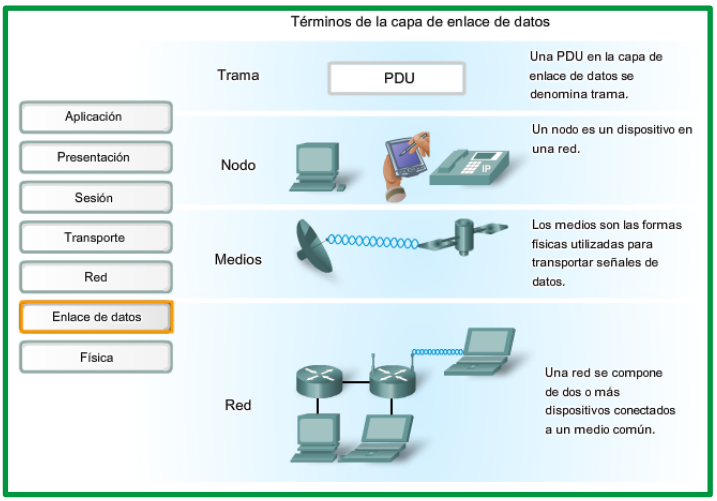


Figura 57: Términos de la capa de enlace de datos.

Los métodos de control de acceso al medio descritos en los protocolos de capa de enlace de datos definen los procesos por los cuales los dispositivos de red pueden acceder a los medios de red y transmitir marcos en diferentes entornos de red.

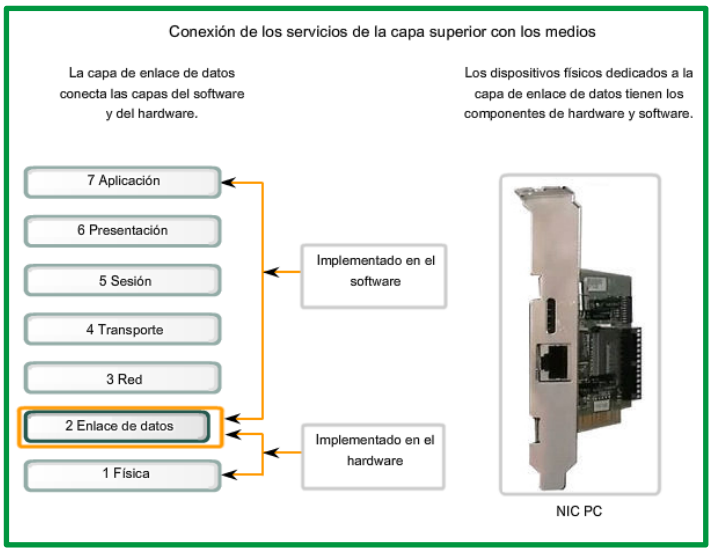


Figura 58: Conexión entre la capa física y capa superioriores.

Un nodo, que es un dispositivo final utiliza un adaptador para hacer la conexión a la red. Por ejemplo: para conectarse a una LAN, el dispositivo usaría la tarjeta de interfaz de red (NIC) para conectarse a los medios LAN. El adaptador administra la trama y el control de acceso a los medios.

La descripción de una trama es un elemento clave de cada protocolo de capa de enlace de datos. Los protocolos de capa de enlace de datos requieren información de control para permitir que los protocolos funcionen. La información de control puede indicar:

- Qué nodos están en comunicación con otros
- Cuando comienza y cuándo termina la comunicación entre nodos individuales
- Qué errores se producen mientras los nodos se comunican
- Qué nodos se comunicarán luego

La Capa de enlace de datos prepara un paquete para transportar a través de los medios locales encapsulándolo con un encabezado y un tráiler para crear una trama. A diferencia de otros PDU que han sido analizados en este curso, la trama de la capa de enlace de datos incluye:

- **Datos**: El paquete desde la Capa de red
- **Encabezado**: contiene información de control como direccionamiento y está ubicado al comienzo del PDU
- **Tráiler**: contiene información de control agregada al final del PDU

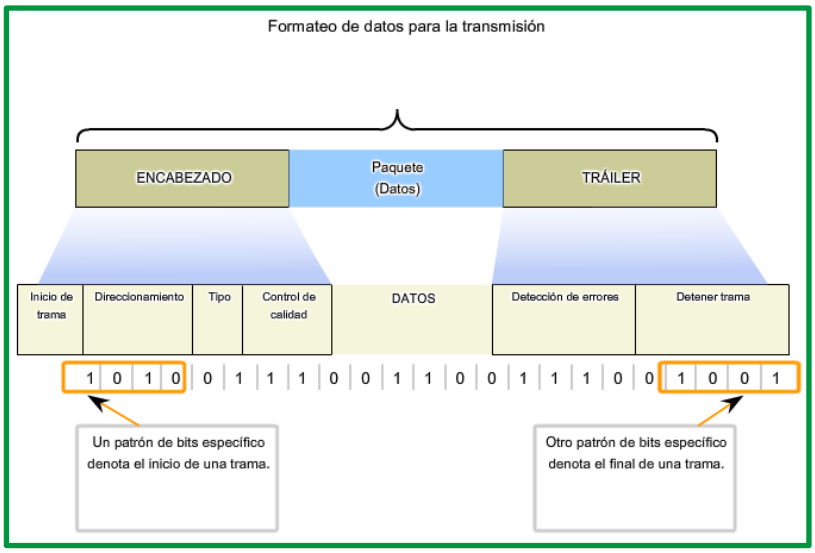


Figura 59: Trama en la capa enlace de dato.

Subcapas de enlace de datos

Para sostener una gran variedad de funciones de red, la capa de enlace de datos a menudo se divide en dos subcapas: una subcapa superior y una subcapa inferior.

La subcapa superior define los procesos de software que proveen servicios a los Protocolos de capa de red.

La subcapa inferior define los procesos de acceso a los medios realizados por el hardware.

Separar la Capa de enlace de datos en subcapas permite a un tipo de trama definida por la capa superior acceder a diferentes tipos de medios definidos por la capa inferior. Tal es el caso en muchas tecnologías LAN, incluida Ethernet.

Las dos subcapas comunes de LAN son:

Control de enlace lógico

El control de enlace lógico (LLC) coloca información en la trama que identifica qué protocolo de capa de red está siendo utilizado por la trama. Esta información permite que varios protocolos de la Capa 3, tales como IP e IPX, utilicen la misma interfaz de red y los mismos medios.

Control de acceso al medio

El control de acceso al medio (MAC) proporciona a la capa de enlace de datos el direccionamiento y la delimitación de datos de acuerdo con los requisitos de señalización física del medio y al tipo de protocolo de capa de enlace de datos en uso.

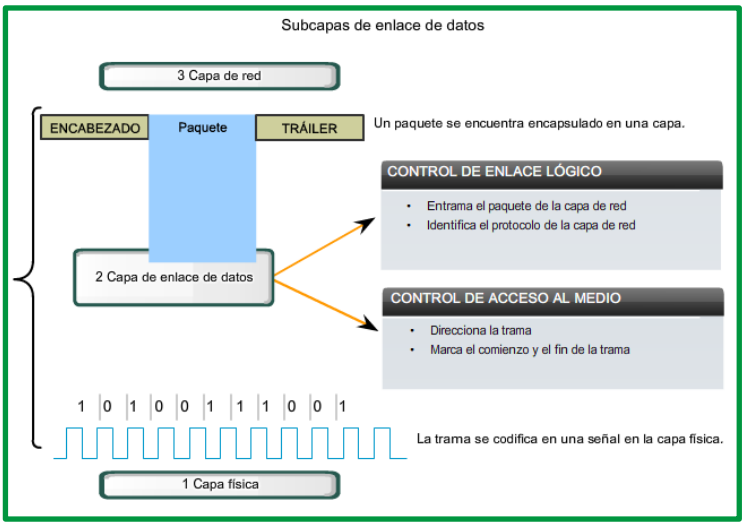


Figura 60: Subcapas de enlace de datos.

Capa de Red:

El nivel de red se ocupa de encaminar los datos hacia su destino estableciendo el camino de transmisión. Este nivel elige la ruta más adecuada para que los paquetes, bloques de datos en los que el nivel de red divide los mensajes, lleguen a su destino. Para ello, se establecen prioridades para los paquetes y varias rutas alternativas.

Los routers o encaminadores son los dispositivos que almacenan y reenvían paquetes encaminándolos hacia el siguiente nodo de interconexión por el que el paquete ha de pasar para alcanzar su destino entre distintas redes. Cada nodo necesita un tiempo para procesar los paquetes que le llegan. Cuando hay gran cantidad de tráfico en la red, unos paquetes obstruyen a otros generando cuellos de botella en los puntos más sensibles. Esta congestión en un nodo se propaga rápidamente a las zonas vecinas. Si llega un nuevo paquete cuando se está procesando otro, el nivel de red proporciona algún mecanismo que impida la pérdida de información, bien rechazando los nuevos paquetes que llegan o controlando los nodos vecinos para que no envíen más paquetes.

La Capa de red o Capa 3 de OSI provee servicios para intercambiar secciones de datos individuales a través de la red entre dispositivos finales identificados. Para realizar este transporte de extremo a extremo la Capa 3 utiliza cuatro procesos básicos:

- Direccionamiento,
- Encapsulamiento,
- Enrutamiento, y
- Desencapsulamiento.

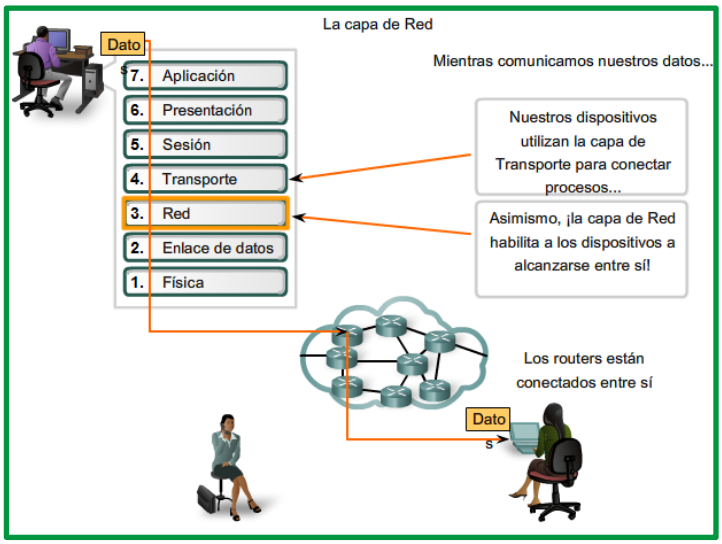


Figura 61: Capa de red.

El nivel de red se encarga de enviar paquetes a destinatarios que no están en la misma red. La red destino podría usar un sistema de direccionamiento distinto al de la red de origen. También es posible que la segunda red no admita paquetes de las mismas dimensiones que la primera. En general, en este nivel se resuelven los problemas generados por redes heterogéneas.

Algunas de las funciones del nivel de red son:

- Encaminamiento: elegir la ruta más adecuada para que el bloque de datos de este nivel paquete) llegue a su destino.
- Tratamiento de la congestión evitando cuellos de botella en la red.
- Resolución de problemas relacionados con redes heterogéneas: sistemas de direccionamiento distintos, paquetes de distintas dimensiones, etc.

Capa de transporte:

La capa de Transporte permite la segmentación de datos y brinda el control necesario para reensamblar las partes dentro de los distintos streams de comunicación. Las responsabilidades principales que debe cumplir son:

- Seguimiento de la comunicación individual entre aplicaciones en los hosts origen y destino,
- Segmentación de datos y gestión de cada porción,
- Reensamble de segmentos en flujos de datos de aplicación, e
- Identificación de las diferentes aplicaciones.

El nivel de transporte se ocupa de la comunicación extremo a extremo (peer to peer) entre equipos de una red; es decir, la comunicación entre una aplicación emisora y otra receptora. Este nivel se encarga de que los datos enviados y recibidos lleguen en orden, sin duplicar y sin errores. El nivel de transporte ofrece tanto servicios orientados a conexión como no orientados a conexión.

La misión del nivel de transporte consiste en aceptar los datos de la capa de sesión, fraccionarlos de modo que se puedan enviar a los niveles inferiores y asegurarse de que llegan correctamente

al nivel de transporte del destinatario que puede estar o no en la misma red que el emisor de los datos. El nivel de transporte permite varias conexiones de aplicación en una única conexión de red. Es decir, multiplexa la comunicación de varias aplicaciones en un mismo instante. Para que esto pueda ocurrir, el direccionamiento a nivel de transporte debe garantizar la identificación de diferentes aplicaciones. Entre las funciones del nivel de transporte están:

- Aceptar datos del nivel de sesión y fraccionarlos para enviarlos por la red.
- Asegurarse de que los datos transmitidos llegan correctamente al receptor.
- Multiplexar conexiones distintas de la capa de sesión de forma transparente al usuario.
- Establecer comunicaciones entre el emisor y el receptor.
- Controlar el flujo de la transmisión entre el emisor y el receptor.

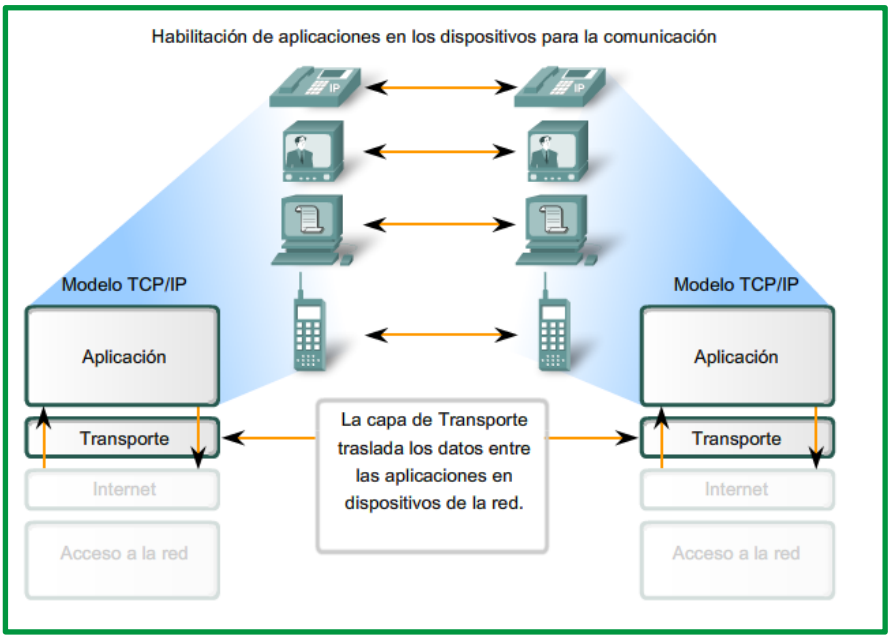


Figura 62: Capa de Transporte traslada los datos en el dispositivo de la red.

Capa de Sesión

El nivel de sesión permite el dialogo eficiente entre el emisor y el receptor estableciendo una sesión (nombre que reciben las conexiones en esta capa), de modo que hace posible el intercambio ordenado de datos en un sentido u otro y controla la desconexión de la comunicación. El nivel de sesión permite agrupar datos de diversas aplicaciones para enviarlos juntos, o incluso, detener la comunicación y restablecer el envío tras realizar algún tipo de actividad.

Como lo indica el nombre de la capa de Sesión, las funciones en esta capa crean y mantienen diálogos entre las aplicaciones de origen y destino. La capa de sesión maneja el intercambio de información para iniciar los diálogos y mantenerlos activos, y para reiniciar sesiones que se interrumpieron o desactivaron durante un periodo de tiempo prolongado.

La mayoría de las aplicaciones, como los exploradores Web o los clientes de correo electrónico, incorporan la funcionalidad de las capas 5, 6 y 7 del modelo OSI.

Algunas de las funciones del nivel de sesión son:

- Establecimiento de la sesión y creación de un buzón donde se recibirán mensajes procedentes de las capas inferiores.
- Intercambio de datos entre los buzones del emisor y el receptor siguiendo unas reglas de diálogo.
- Control del diálogo: Determinar si la comunicación será o no bidireccional y simultánea.
- Tratamiento de las interrupciones por fallos en la red.

Capa de Presentación

La capa de Presentación tiene tres funciones primarias:

- Codificación y conversión de datos de la capa de aplicación para garantizar que los datos del dispositivo de origen puedan ser interpretados por la aplicación adecuada en el dispositivo de destino.
- Compresión de los datos de forma que puedan ser descomprimidos por el dispositivo de destino.
- Encriptación de los datos para transmisión y descifre de los datos cuando se reciben en el destino.

El nivel de presentación se encarga de definir los formatos de los datos y si es necesario, comprimirlos o codificarlos antes de su envío.

Capa de Aplicación

La capa de Aplicación, Capa siete, es la capa superior de los modelos OSI y TCP/IP. Es la capa que proporciona la interfaz entre las aplicaciones que utilizamos para comunicarnos y la red subyacente en la cual se transmiten los mensajes. Los protocolos de capa de aplicación se utilizan para intercambiar los datos entre los programas que se ejecutan en los hosts de origen y destino. Existen muchos protocolos de capa de aplicación y siempre se desarrollan protocolos nuevos.

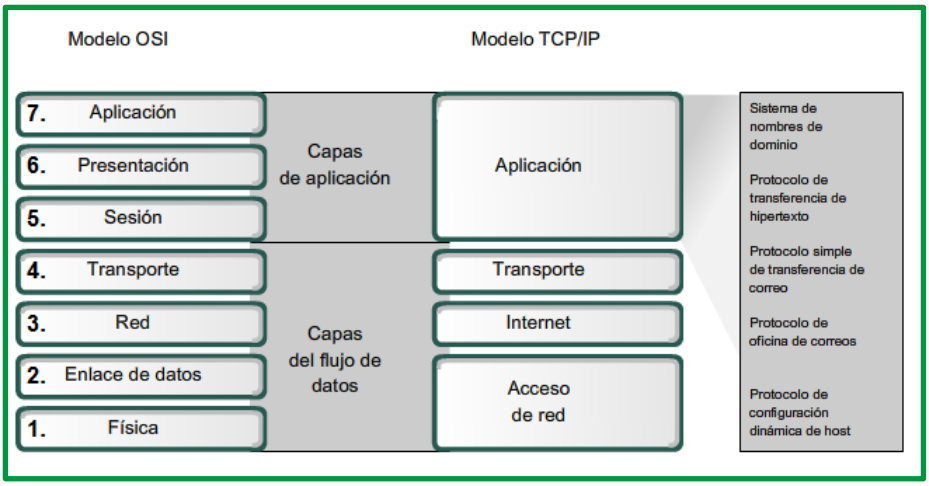


Figura 63: Comparación de la capa de aplicación y del flujo de datos, modelo OSI y TCP/IP.

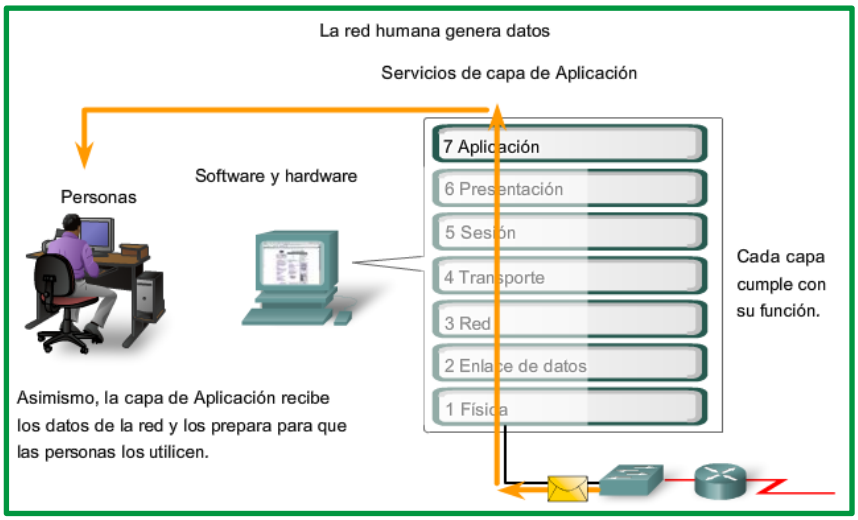


Figura 64: Capa de Aplicación ofrece servicios que son abstracto para el usuario final.

Cuando dos aplicaciones de los usuarios que desean comunicarse residen en el mismo ordenador, la comunicación se realiza utilizando las funciones que les ofrece el sistema operativo. Sin embargo, si las aplicaciones residen en ordenadores distintos, el nivel de aplicación disparará los mecanismos adecuados para producir la conexión entre ellos, sirviéndose de los servicios de las capas inferiores.

En este nivel se definen los protocolos que utilizan las aplicaciones de los usuarios para comunicarse. Estos protocolos atienden las peticiones de las aplicaciones que requieren comunicación a través de la red y permiten que varias aplicaciones compartan la red. Cada una de las diferentes aplicaciones de usuario lleva asociado un protocolo específico del nivel de aplicación.

El nivel de aplicación proporciona diferentes servicios a las aplicaciones. Entre ellos se pueden destacar:

- correo electrónico
- control de seguridad
- transferencia de ficheros
- emulación de terminales
- carga de programas a través de líneas de comunicaciones
- etc.

Modelo de referencia protocolo de control de transmisión/protocolo de Internet TCP/IP

El modelo de protocolo en capas para comunicaciones de internetwork se creó a principios de la década de los setenta y se conoce con el nombre de modelo de Internet. Define cuatro categorías de funciones que deben tener lugar para que las comunicaciones sean exitosas. La arquitectura de la suite de protocolos TCP/IP sigue la estructura de este modelo. Por esto, es común que al modelo de Internet se lo conozca como modelo TCP/IP.

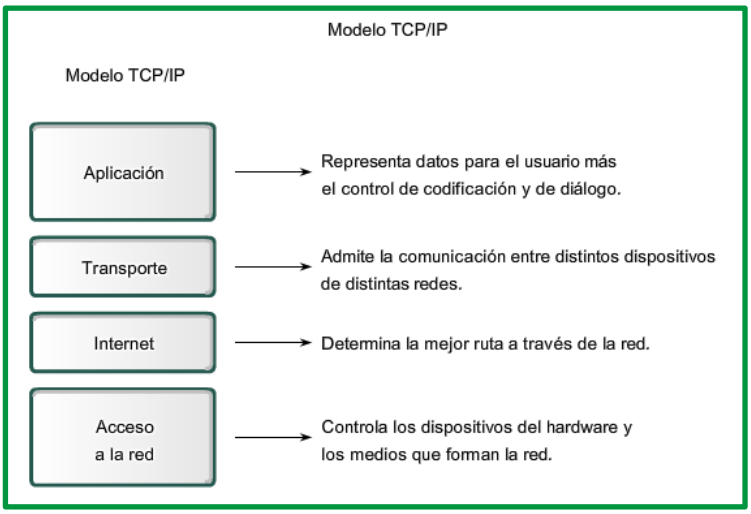


Figura 65: Modelo TCP/IP

Como se podrá observar en la gráfica, el Modelo TCP/IP está conformado por cuatro capas o niveles:

- **Aplicación**
- **Transporte**
- **Internet**
- **Acceso a la red**

La mayoría de los modelos de protocolos describen un stack de protocolos específicos del proveedor. Sin embargo, puesto que el modelo TCP/IP es un estándar abierto, una compañía no controla la definición del modelo. Las definiciones del estándar y los protocolos TCP/IP se explican en un foro público y se definen en un conjunto de documentos disponibles al público. Estos documentos se denominan Solicitudes de comentarios (RFCS). Contienen las especificaciones formales de los protocolos de comunicación de datos y los recursos que describen el uso de los protocolos.

Las RFC (Solicitudes de comentarios) también contienen documentos técnicos y organizacionales sobre Internet, incluyendo las especificaciones técnicas y los documentos de las políticas producidos por el Grupo de trabajo de ingeniería de Internet (IETF).

El modelo TCP/IP describe la funcionalidad de los protocolos que forman la suite de protocolos TCP/IP. Esos protocolos, que se implementan tanto en el host emisor como en el receptor, interactúan para proporcionar la entrega de aplicaciones de extremo a extremo a través de una red.

Un proceso completo de comunicación incluye estos pasos:

1. Creación de datos a nivel de la capa de aplicación del dispositivo final origen.
2. Segmentación y encapsulación de datos cuando pasan por la stack de protocolos en el dispositivo final de origen.
3. Generación de los datos sobre el medio en la capa de acceso a la red de la stack.
4. Transporte de los datos a través de la internetwork, que consiste de los medios y de cualquier dispositivo intermediario.

5. Recepción de los datos en la capa de acceso a la red del dispositivo final de destino.
6. Desencapsulación y rearmado de los datos cuando pasan por la stack en el dispositivo final.
7. Traspaso de estos datos a la aplicación de destino en la capa de aplicación del dispositivo final de destino.

Unidad de datos y encapsulación

Mientras los datos de la aplicación bajan al stack del protocolo y se transmiten por los medios de la red, varios protocolos le agregan información en cada nivel. Esto comúnmente se conoce como proceso de encapsulación.

La forma que adopta una sección de datos en cualquier capa se denomina Unidad de datos del protocolo (PDU). Durante la encapsulación, cada capa encapsula las PDU que recibe de la capa inferior de acuerdo con el protocolo que se utiliza. En cada etapa del proceso, una PDU tiene un nombre distinto para reflejar su nuevo aspecto.

- **Datos**: el término general para las PDU que se utilizan en la capa de aplicación.
- **Segmento**: PDU de la capa de transporte.
- **Paquete**: PDU de la capa de Internetwork.
- **Trama**: PDU de la capa de acceso a la red.
- **Bits**: una PDU que se utiliza cuando se transmiten físicamente datos a través de un medio.

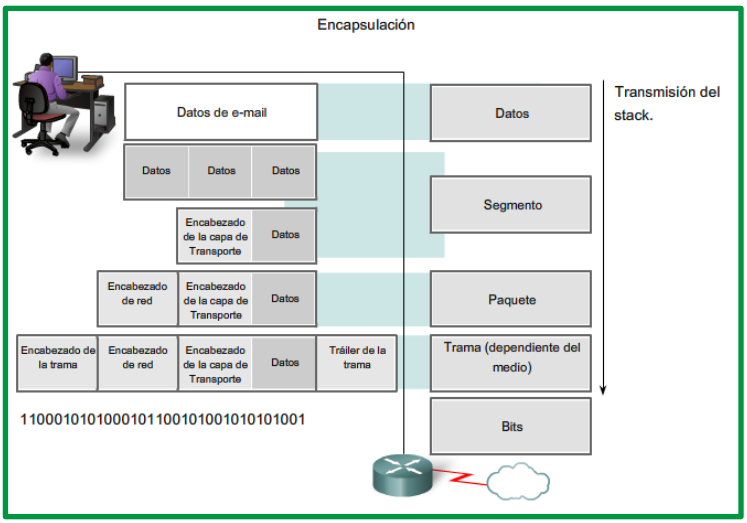


Figura 66: Encapsulación.

Proceso de envío y recepción:

Cuando se envían mensajes en una red, el stack del protocolo de un host funciona desde arriba hacia abajo; mientras el proceso de recepción se invierte en el host receptor. Los datos se encapsulan mientras suben al stack hacia la aplicación del usuario final.

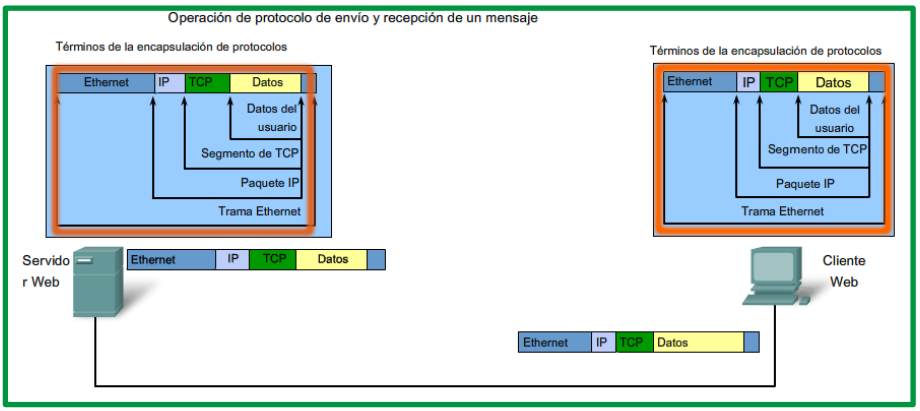


Figura 67: términos de la encapsulación de protocolos de envío y recepción de un mensaje.

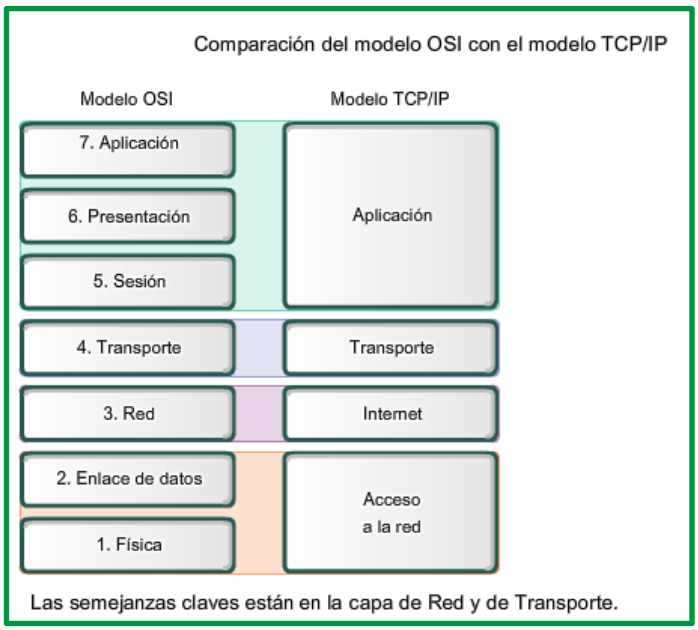


Figura 68: Comparación de capas entre el modelo OSI con el modelo TCP/IP

A continuación, se presenta un resumen de las principales características de cada nivel:

Aplicación: en este nivel la comunicación es entre procesos o aplicaciones que manejan datos de usuario y se los deben comunicar a otros procesos o aplicaciones en otro punto de la red. Se trata del nivel más alto de la arquitectura, comparable a las tres capas de mayor numeración del Modelo OSI, aunque muchas veces sería imposible establecer una relación directa entre protocolos en este nivel con funcionalidades específicas de una capa OSI. Protocolos tales como SMTP para transporte de mensajes de correo electrónico, FTP para transferencia de archivos, SSH para conexiones remotas seguras y HTTP para navegación en la web, operan en este nivel.

Transporte: es el nivel de comunicación entre las máquinas en red que constituyen los extremos finales de la comunicación. Las mismas pueden encontrarse en redes diferentes conectadas a través de routers, o en la misma red. Los protocolos de este nivel, TCP y UDP, ofrecen a los del nivel superior una interfaz de acceso a la red uniforme, sin que importe el tipo de conexión o red subyacente. Se les asocia funcionalidades relacionadas con el control de error y control de flujo, aunque TCP también permite manejar una conexión, porque es un protocolo del tipo orientado a la conexión. Es decir que TCP se encarga de brindar confiabilidad, abrir, mantener y cerrar

conexiones solicitadas por aquellos protocolos de nivel superior que requieren sus servicios. Para ello, es capaz de manejar datos fuera de orden, errados o duplicados. Su funcionalidad incluye el control de congestión y el manejo de paquetes perdidos. Protocolos tales como HTTP apoyan su funcionalidad en TCP. Por su parte, UDP ofrece un servicio sin conexión, apto para aplicaciones transaccionales, como es el caso de DNS. Tanto TCP como UDP incluyen un esquema de direccionamiento para identificar aplicaciones. Se trata de campos de encabezado, de 16 bits, conocidos como números de puerto.

Red: existe un único protocolo a este nivel y su función es la de lograr la interconexión de redes. IP cuenta con capacidad de manejo de datagramas o paquetes y su misión es que los mismos se muevan hacia el destino, a través de diversas redes. El servicio de transmisión de datagramas IP es un servicio sin conexión, no confiable, pero que permite lograr uno de los objetivos más importantes de manera sencilla: la interconectividad. Como su principal trabajo es el ruteo, en su versión más antigua, el protocolo IPv4 posee un esquema de direccionamiento de tipo jerárquico, de 32 bits, conocido como esquema de direcciones IP. La versión más moderna IPv6 cuenta con un espacio de direcciones mucho más grande, de 128 bits. El servicio de ruteo es tipo salto a salto o hop-by-hop, con comunicación entre sistemas conectados directamente hasta llegar al router más cercano al destino final. IP puede cargar mensajes de muchos protocolos del nivel superior, identificados con un campo especial en el encabezado, denominado campo de número de protocolo, que le permite realizar multiplexado para poder entregar de manera correcta el mensaje encapsulado. Entre los protocolos encapsulados por IP, podemos mencionar: el Protocolo de Mensajes de Control de Internet (ICMP, Internet Control Message Protocol), y los protocolos TCP y UDP.

Enlace: es el nivel que atiende las cuestiones relacionadas con el tipo de red local sobre la que se dirige la comunicación. En términos comparativos, los protocolos en este nivel de la pila se ubican en las Capas de Enlace y Física del modelo OSI. Es decir que aquí se manejan los detalles del medio de comunicación sobre el que se transmitirán y recibirán los datagramas generados por IP entre dos máquinas diferentes conectadas indirectamente o sobre el mismo enlace. La funcionalidad de los protocolos de este nivel puede desarrollarse en hardware, por ejemplo, en las placas de red, y en software. Antes de enviar los datagramas sobre el medio físico específico, estos serán acondicionados con el agregado de un encabezado generado por protocolos de este nivel, por ejemplo, para agregar algún tipo de direccionamiento con significado local, a diferencia de IP cuyo direccionamiento es de significado global. Muchos protocolos de este nivel también agregan al final un campo para control de errores. Uno de los protocolos más antiguos que operan en este nivel es el Protocolo de Resolución de Direcciones (ARP, Address Resolution Protocol). En el caso de redes de acceso múltiple, este protocolo trabaja en conjunto con el protocolo IPv4, para relacionar direcciones IP con las correspondientes direcciones del nivel de enlace.

Estándares y organismos de estandarización

Toda vez que se enfrente el estudio de redes de datos, se deberán analizar estándares que regulan su funcionalidad y organizaciones que son las responsables de la generación de esos estándares. La necesidad de interconectar equipos con diferentes especificaciones de hardware

o software pone en evidencia la importancia de estos estándares, ellos describen protocolos y tecnologías.

Se definen como sistemas abiertos, aquellos que son capaces de interactuar con otros de diferente tecnología. Estos sistemas se desarrollan en base a estándares universales, a diferencia de los sistemas propietarios que sólo pueden interactuar con otros sistemas similares. La definición de un estándar universal permite, por ejemplo, que equipos de diferentes fabricantes puedan compartir un entorno.

Para poder desarrollar estándares universales, se precisan organizaciones que coordinen las discusiones y la publicación de la documentación.

Organismo de estandarización:

- **Organización Internacional para Estandarización (ISO, International Organization for Standardization).**

  Esta organización no gubernamental fue creada en 1946. Sus miembros son organismos nacionales de máxima representatividad en el tema de estandarización, aceptándose sólo un miembro por país. http://www.iso.org/ .

- **Instituto Nacional Americano de Estándares (ANSI, American National Standards Institute).**

  Responsable de coordinar y publicar los estándares de tecnología de la información y computación en Estados Unidos. Es miembro de la ISO. Por ejemplo, ANSI C es un estándar para el lenguaje de programación C. http://www.ansi.org/ .

- **Instituto de Ingenieros Electricistas y Electrónicos (IEEE, Institute of Electrical and Electronics Engineers).**

  Organización de profesionales de ingeniería eléctrica y electrónica. Uno de los estándares más conocidos de la IEEE es el proyecto IEEE 802, que permitió el desarrollo de tecnologías LAN tipo Ethernet y WiFi. http://www.ieee.org/ .

- **Alianza de Industrias Electrónicas (EIA, Electronic Industries Alliance).**

  Asociación internacional de industrias cuyos estándares más conocidos se refieren al cableado de redes. http://www.eia.org/ .

- **Unión Internacional de Telecomunicaciones – Sector de Estandarización para Telecomunicaciones (ITU-T, International Telecommunication Union – Telecommunication Standardization Sector)**.

  Organización internacional para desarrollo de estándares para la industria de las telecomunicaciones. https://www.itu.int/en/Pages/default.aspx .

- **IETF (Internet Engineering Task Force).**

  Este Grupo de Trabajo de Ingeniería de Internet, es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad. Fue

creada en EE.UU. en 1986. El IETF es mundialmente conocido por ser la entidad que regula las propuestas y los estándares de Internet, conocidos como RFC (Request For Comments).

- **Sociedad de Internet (ISOC).**

  Es responsable de promover el desarrollo, la evolución y el uso abiertos de Internet en todo el mundo.

- **Consejo de Arquitectura de Internet (IAB).**

  Es responsable de la administración y el desarrollo general de los estándares de Internet.

- **Grupo de trabajo de investigación de Internet (IRTF).**

  Está enfocado en la investigación a los protocolos de Internet y TCP/IP

- **TIA (Telecommunications Industry Association).**

  La Asociación de la Industria de las Telecomunicaciones Organización formada por representantes de las industrias más importantes del sector de las telecomunicaciones, han desarrollado estándares a nivel internacional relacionados con las redes en colaboración con ANSI y la antigua EIA.

- **ETSI (European Telecommunications Standards Institute).**

  Creado en 1988, ETSI es una organización independiente sin ánimo de lucro que produce estándares aplicables globalmente para las tecnologías de la información y comunicación.

- **Comité Europeo de Normalización (CEN).**

  El CEN fue fundado en 1961. Sus miembros nacionales trabajan juntos para desarrollar los estándares europeos (EN) en varios sectores.

- **W3C (World Wide Web Consortium, http://www.w3c.org/)**.

  Se encarga de nuevos estándares para aplicaciones web. Por ejemplo, HTML, CSS, XML, SOAP, etc.

- **ICANN**: **la Internet Corporation for Assigned Names and Numbers (ICANN).**

  Es un organismo sin fines de lucro con base en los Estados Unidos que coordina la asignación de direcciones IP, la administración de nombres de dominio utilizados por DNS y los identificadores de protocolo o los números de puerto utilizados por los protocolos TCP y UDP. ICANN crea políticas y tiene una responsabilidad general sobre estas asignaciones.

- **IANA: la Internet Assigned Numbers Authority (IANA).**

  Es un departamento de ICANN responsable de controlar y administrar la asignación de direcciones IP, la administración de nombres de dominio y los identificadores de protocolo para ICANN.

Estándares:

Los diferentes estándares desarrollados y en desarrollo por los organismos internacionales están publicados en sitios web donde se pueden verificar el estado de los mismo, se detallan varios los sitios de consulta de referencia:

- https://standards.ieee.org/standard/index.html
- https://www.iso.org/standards.html
- https://www.ansi.org/
- https://www.itu.int/es/ITU-T/Pages/default.aspx
- https://www.w3.org/

Es importante mencionar que dentro del estudio de las diferentes capas o niveles de estudio intervienen varios estándares desarrolladores por diferentes organismos internacionales mismo que serán detallado en cada capa, a continuación, se describe como ejemplo los estándares aplicados en la capa de enlace de datos:

Estándares para la capa de enlace de datos

ISO:	HDLC (Control de enlace de datos de alto nivel)
IEEE:	802.2 (LLC), 802.3 (Ethernet) 802.5 (Token Ring) 802.11(Wireless LAN [LAN inalámbrico])
ITU:	Q.922 (Estándar de Frame Relay) Q.921 (Estándar de enlace de datos ISDN) HDLC (Control de enlace de datos de alto nivel)
ANSI:	3T9.5 ADCCP (Protocolo de control de comunicación avanzada de datos)

Figura 69: Estándares aplicados en la capa de enlace de datos.

A continuación, se detalla el grupo de trabajo y grupos de estudio de IEEE 802

- **802.1** Higher Layer LAN Protocols Working Group (Grupo de trabajo de protocolos LAN de capa superior).

- **802.3** Ethernet Working Group (Grupo de trabajo de Ethernet).

Tipos de Ethernet

Tipo de Ethernet	Ancho de banda	Tipo de cable	Duplex	Distancia máxima
10Base-5	10 Mbps	Coaxial thicknet	Half	500 m
10Base-2	10 Mbps	Coaxial thinnet	Half	185 m
100Base-TX	10 Mbps	UTP Cat3/Cat5	Half	100 m
100Base-TX	100 Mbps	UTP Cat5	Half	100 m
100Base-TX	200 Mbps	UTP Cat5	Full	100 m
100Base-TX	100 Mbps	Fibra multimodo	Half	400 m
1000Base-T	200 Mbps	Fibra multimodo	Full	2 km
1000Base-TX	1 Gbps	UTP Cat5e	Full	100 m
1000Base-SX	1 Gbps	UTP Cat6	Full	100 m
1000Base-LX	1 Gbps	Fibra multimodo	Full	550 m
10GBase-CX4	1 Gbps	Fibra monomodo	Full	2 km
10GBase-T	10 Gbps	Twinaxial	Full	100 m
10GBase-LX4	10 Gbps	UTP Cat6a/Cat7	Full	100 m
10GBase-LX4	10 Gbps	Fibra multimodo	Full	300 m
10 Mbps	10 Gbps	Fibra monomodo	Full	10 km

Figura 70: Estándar 802.3

Para más información revisar documento en :
https://drive.google.com/file/d/1vP1D6svW9Bdyf7MBM7rkBBB5oAsyOlHn/view?usp=sharing

- **802.11** Wireless LAN Working Group (Grupo de trabajo de LAN inalámbrica)
- **802.15** Wireless Personal Area Network (WPAN) Working Group (Grupo de trabajo de red de área personal inalámbrica [WPAN])
- **802.16** Broadband Wireless Access Working Group (Grupo de trabajo de acceso inalámbrico de banda ancha)
- **802.18** Radio Regulatory TAG (Grupo de asesoría técnica sobre normativas de radio)
- **802.19** Wireless Coexistence Working Group (Grupo de trabajo de coexistencia inalámbrica)
- **802.21** Media Independent Handover Services Working Group (Grupo de trabajo de servicios para la transición independiente del medio)
- **802.22** Wireless Regional Area Networks (Grupo de trabajo de redes de área regional inalámbricas)
- **802.24** Smart Grid TAG (Grupo de asesoría técnica sobre redes inteligentes).

Estándares ANSI/EIA/TIA.

ANSI/TIA/EIA-568: Los estándares para definir normas para el cableado estructurado es la ANSI/EIA/TIA 508, se publicó por primera vez en 1991, posteriormente se realizan revisiones en 1995, en 2001 y en 2009. La norma considera la asignación de pines/pares para cable de par trenzado equilibrado de 100 Ω y 8 conductores.

Par trenzado de 4 pares:

UTP (UnshleldedTwistedPair): Par trenzado sin blindaje) -100 ohms, 22/24 AWG.

STP (ShieldedTwistedPair) : Par trenzado con blindaje -150 ohms, 22/24 AWG

Fibra Optica multimodo62.5/125 y 50/125 µmde 2 fibras

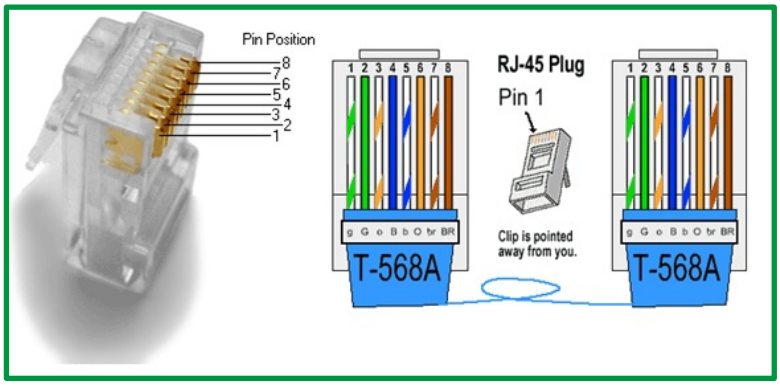


Figura 71: Conector rj45, estándar 568A

- **ANSI/EIA/TIA-568-A**: Regula todo lo concerniente a sistemas de cableado estructurado para edificios comerciales.
- **ANSI/EIA/TIA-568-B**: Especifica un sistema de cableado genérico a fin de proveer un sistema de transporte de información con redes externas por un medio común y establece los requisitos de funcionamiento para dicho sistema de cableado.
- **ANSI/EIA/TIA-568-C**: Es una revisión del ANSI/TIA/EIA 568-B, publicado entre 2001 y 2005. El nuevo estándar consolida los documentos centrales de las recomendaciones originales y todos los "adendum", pero cambia la organización, generando una recomendación "genérica" o "común" a todo tipo de edificios.
- **ANSI/TIA/EIA-570-A**: Normas de Infraestructura Residencial de Telecomunicaciones
- **ANSI/TIA/EIA-606-A**: Normas de Administración de Infraestructura de Telecomunicaciones en Edificios Comerciales.
- **ANSI/TIA/EIA-607**: Requerimientos para instalaciones de sistemas de puesta a tierra de Telecomunicaciones en Edificios Comerciales.
- **ANSI/TIA/EIA-758**: Norma Cliente-Propietario de cableado de Planta Externa de Telecomunicaciones.

Estándares de protocolos de comunicaciones.

Es el conjunto de normas o standard que especifican el método para establecer conexiones que permitan enviar y recibir de un extremo a otro. Los protocolos son reglas de comunicación que permiten el flujo de información entre equipos que manejan lenguajes distintos, no existe un único protocolo de red, y es posible que en un mismo ordenador coexistan instalados varios protocolos (IP, IPX/SPX, X25, X21, Frame relay, NetBIOS, NetBEUI , Apple Talk , TCP, entre otros).

A continuación, se hace una comparación de las referencias de protocolos aplicadas a nivel del modelo de referencia OSI y TCP/IP.

MODELO OSI	PROTOCOLOS	MODELO TC/IP	PROTOCOLOS
Capa de aplicación	HTTP, DNS, SMTP, SNMP, FTP, Telnet, SSH y SCP, NFS, RTSP, Feed, Webcal , POP3, IMAP	**Capa de aplicación**	HTTP, DNS, SMTP, SNMP, FTP, Telnet, SSH y SCP, NFS, RTSP, Feed, Webcal ,

Capa de presentación	XDR, ASN.1, SMB, AFP		POP3, IMAP
Capa de sesión	TLS, SSH, ISO 8327 / CCITT X.225, RPC, NetBIOS		
Capa de transporte	TCP, UDP, RTP, SCTP, SPX	**Capa de transporte**	TCP, UDP, RTP, SCTP
Capa de red	IP, ICMP, IGMP, X.25, CLNP, ARP, RARP, BGP, OSPF, RIP, IGRP, EIGRP, IPX, DDP	**Capa de internet**	IP, ICMP, IGMP, X.25, CLNP, ARP, RARP, BGP, OSPF, RIP, IGRP, EIGRP, IPX, DDP
Capa de enlace de datos	Ethernet, Token Ring, RDSI, ATM, IEEE 802.11, FDDI	**Capa de acceso a la red**	Ethernet, Token Ring, RDSI, ATM, IEEE 802.11, FDDI
Capa física	cable, radio, fibra óptica		

Tabla 1: Comparación de protocolos de comunicación en modelo OSI y TCPI

Tecnologías utilizadas en las redes de comunicaciones

La evolución de las redes de comunicaciones desde sus inicios ha aplicado y optimizado el uso eficiente de las diversas tecnologías que han permitido mejorar el rendimiento, transmitiendo información cada vez con mayor alcance y rapidez.

Se puede clasificar las tecnologías aplicada a las redes de comunicaciones en inalámbrica y cableada:

Tecnologías inalámbricas

Las tecnologías de comunicación inalámbricas se han desarrollado para la transferencia de datos entre dos o más puntos sin la necesidad de contar con una infraestructura física entre ellas. Además, tiene varias ventajas, como su bajo costo de implementación, despliegues rápidos y movilidad, que las hacen muy atractivas para su uso en redes de potencia inteligentes.

- **LAN inalámbrica**

  Proporciona una comunicación de punto a punto y punto a multipunto de alta velocidad. Esta tecnología se adoptó bajo el estándar IEEE 802.11 (WiFi), el cual permite que varios usuarios ocupen la misma banda de frecuencias con mínima interferencia entre ellos.

  Las diversas versiones del estándar 802.11 son: IEEE 802.11b, 802.11a, 802.11g, 802.11n y 802.11i, los cuales presentan velocidades de datos desde los 11 Mbps a los 600 Mbps aproximadamente, en las bandas de frecuencia de 2.4 GHz y 5.8 GHz. Emplean las técnicas de modulación DSSS y OFDM. Además, el 802.11i conocido como WPA- 2 es empleado para mejorar la seguridad cibernética en las redes LAN inalámbricas.

  WiFi permite muchas aplicaciones dentro del contexto de automatización, protección y control de recursos. Entre las aplicaciones más destacadas basadas en la norma IEC 61850, se encuentran: fortalecimiento de la protección del transformador, enlace

redundante para el sistema de distribución automatizado, protección de línea eléctrica, y control y seguimiento de fuentes de energía renovables remotas.

Por otra parte, esta tecnología presenta algunas limitaciones como: mala disponibilidad de la señal inalámbrica, se ve afectada por las radiaciones electromagnéticas en lugares de alta tensión y no menos importante, las interferencias ocasionadas por las frecuencias de radio que afectan el funcionamiento de los equipos.

- **WiMAX**

  Una red WiMAX proporciona un ancho de banda de 5 MHz con una velocidad de hasta 70 Mbps a una distancia de 48 Km. Para la comunicación en bandas fijas se han asignado las bandas de frecuencia de 3.5 y 5.8 GHz, mientras que para la comunicación móvil se han asignado las bandas de 2.3, 2.5 y 3.5 GHz. Los espectros con licencias brindan mayor potencia y distancia de transmisión, lo que los hace más adecuado para la comunicación a larga distancia. Está regido por la norma IEEE 802.16d (fijo) y 802.16e (datos móviles). WiMAX ofrece una serie de capacidades, además de su excelente latencia, que hacen de esta tecnología una buena opción para el control de aplicaciones. Posee modulación adaptativa y control de potencia. Igualmente, la red WiMAX permite a un operador priorizar el tráfico de datos mediante lo que se le conoce como calidad de servicio QoS.

  Las aplicaciones que proporciona WiMAX en el contexto de redes inteligentes son:

  - ✓ Redes inalámbricas de lectura automática (WMAR), gracias a la gran cobertura y altas velocidades que presenta.
  - ✓ Proporciona los precios en tiempo real a los consumidores conectados a la red de distribución eléctrica gracias a su buena latencia.
  - ✓ Detección de interrupción y restauración.
  - ✓ Las limitaciones que presentan la implementación de una red WiMAX son:
  - ✓ El costo de la construcción de una torre para WiMAX es relativamente alto, ya que ésta debe hacerse de manera óptima para cumplir con la calidad de servicio.
  - ✓ Las frecuencias por encima de 10 GHz no pueden penetrar a través de obstáculos.

- **Tecnología celular**

  Es una red de radio distribuida en una extensa zona terrestre, atendida por un transceptor con una ubicación fija conocida como estación base. Incluye la tecnología GSM, 2G, 3G, 4G, LTE y 5G. Los sistemas de comunicación celular son rápidos que permiten una cobertura de comunicaciones de datos sobre una gran área geográfica. La velocidad de transferencia de datos es de 60-240 Kbps, y la distancia depende de la disponibilidad del servicio celular. La transmisión de datos se intercambia entre célula y célula facilitando el flujo de datos ininterrumpido. La ventaja que ofrece la tecnología celular, es que la infraestructura ya está instalada, por lo que se puede hacer uso de ésta para su implementación. Además, con el reciente crecimiento de la tecnología la velocidad de datos y la calidad de experiencia (QoE) han mejorado mucho.

  Una limitación importante de la tecnología celular es que el establecimiento de la comunicación, por lo general, toma tiempo y la comunicación de datos no es priorizada en caso de eventos especiales.

- **Comunicación satelital**

  Proporciona la comunicación entre múltiples estaciones terrenas, al permitir el acceso a lugares remotos. Este tipo de comunicación funciona como una repetidora, posee la capacidad de recibir y retransmitir información por medio de un dispositivo receptor/ transmisor, llamado transpondedor. Emplea frecuencias diferentes para la recepción y la retransmisión con el propósito de que no se den interferencias entre las señales.

  Entre las aplicaciones de esta tecnología están:

  - ✓ Control y monitoreo remoto, ya que permite una cobertura global. Esto se debe a que en algunos lugares no existe una infraestructura de comunicación por su ubicación lejana.
  - ✓ Integración de los generadores de energía renovable que por lo general se encuentran apartados.
  - ✓ Copia de seguridad cuando las infraestructuras de comunicación terrenas se ven afectadas por algún tipo de desastre naturales o fallas en el sistema.

  La comunicación satelital también presenta algunas limitaciones como:

  - ✓ Los sistemas satelitales poseen un retardo mayor que los otros sistemas de comunicación.
  - ✓ Las características del canal se ven afectadas por las condiciones meteorológicas.
  - ✓ Los altos costos asociados a esta tecnología.

  Comunicación infrarroja.

  Las ondas infrarrojas se usan mucho para la comunicación de corto alcance, La tecnología fue evolucionando hasta llegar a todos los controles remotos de los televisores, grabadores de vídeo y estéreos. Estos controles son direccionales, baratos y fáciles de construir, pero no tiene la capacidad de atravesar objetos sólidos.

  Para la comunicación se usa un “transreceptor” (dispositivo capaz de emitir y detectar luz infrarroja) para enviar datos codificados de acuerdo a un protocolo, y otro transreceptor para recibir estos datos.

Tecnologías cableadas

Las tecnologías cableadas poseen ventajas importantes en referencia a las tecnologías inalámbricas, permiten una mayor velocidad de transmisión a grandes distancias e inmunidad frente a interferencias electromagnéticas. Estas ventajas convierten a esta tecnología en una buena opción para su uso en redes de comunicaciones.

- **PLC (Power Line Communication)**
  La comunicación por líneas eléctricas es una vieja idea que se remonta a principios de 1900, cuando las primeras patentes fueron presentadas en este ámbito. Desde entonces, las empresas de servicios públicos de todo el mundo han estado utilizando esta tecnología para la medición remota y control de carga. PLC es una tecnología para el transporte de datos a través de un conductor utilizado para la transmisión de energía eléctrica, regulado bajo el estándar IEEE P1901.2 y ITU-T.

Se pueden emplear muchos tipos de tecnologías para la comunicación, pero PLC es la única que ofrece un costo menor en cuanto a la infraestructura ya que las líneas ya están disponibles. Otra ventaja del uso de PLC es que permite la comunicación entre los dispositivos de distintas instalaciones eléctricas sólo conectándose al tomacorriente. Desafortunadamente, PLC también lucha con los problemas de atenuación, ruido y distorsión que se encuentran en comunicaciones de RF (radio frecuencias) cuando se comunica a través del cableado de energía eléctrica, la línea de alimentación no se diseñó en su principio para la transmisión de datos, las siguientes limitaciones se deben tomar en cuenta:

- ✓ La variación de la impedancia y la condición de canal.
- ✓ Ruido blanco en la naturaleza.
- ✓ Atenuación correspondiente a la frecuencia utilizada.
- ✓ Cambio de fase (de monofásico a trifásico y viceversa) entre arquitecturas interiores y exteriores.

A continuación, se explicarán las aplicaciones más destacadas de PLC en la red inteligente, en los niveles de alta y media tensión.

Alta Tensión: Las tecnologías PLC que operan a través de líneas de alta tensión de CA y CC de hasta 1.100 KV en la banda de 40-500 KHz permiten velocidades de datos unos pocos cientos de Kbps y juegan un papel importante en las redes de alta tensión debido a su alta fiabilidad, bajo costo y largo alcance.

El ruido que se presenta en una línea de transmisión de alta tensión es causado principalmente por el efecto corona (fenómeno eléctrico que se produce en los conductores de las líneas de alta tensión y se manifiesta en forma de halo luminoso a su alrededor) y otros eventos de fuga o de descarga. En comparación con las líneas de medio y bajo voltaje, las líneas de alta tensión son un mejor medio de comunicación que se caracteriza por una baja atenuación.

PLC además de proporcionar conectividad, también se utilizan para la detección de averías remotas como detección de aislante roto, aislador de cortocircuito y rotura del cable; y para determinar el cambio en la altura sobre el suelo de conductores aéreos horizontales de alta tensión.

Media Tensión: Un aspecto importante para el futuro de las redes inteligentes es la capacidad de transferir datos sobre el estado de la red de media tensión donde la información de los equipos y de las condiciones del flujo de potencia debe ser transmitida entre las subestaciones dentro de la red. Los materiales empleados en la construcción de la infraestructura de la red de media tensión son de hace muchos años, por lo que la detección de averías y la vigilancia se han convertido en un aspecto muy importante hoy en día. Algunas aplicaciones de la comunicación por líneas de media tensión son:

- ✓ Control remoto para la prevención de fenómenos de islas.
- ✓ Verificación de la temperatura de los transformadores.
- ✓ Control de la tensión en el secundario de los transformadores.
- ✓ Encuestas de fallas.
- ✓ Medición de calidad de energía.

- **Fibra óptica**

La fibra óptica presenta importantes características que la hacen ser de uso imprescindible en el entorno de alta tensión, como: su gran capacidad de ancho de banda y su alta inmunidad a las interferencias electromagnéticas y a las radiofrecuencias. La utilización de diferentes longitudes de onda para el tráfico simultaneo ascendente y descendente permite una gran flexibilidad en el enrutamiento y conmutación de señales ópticas. Es por esto que la fibra óptica juega un papel muy importante en los sistemas de comunicación actuales.

Un aspecto muy importante en las redes inteligentes, es el uso de una infraestructura de comunicación con características de latencia excepcionalmente reducidas. La latencia máxima permitida en un sistema de comunicación es de 6 ciclos, o 100 ms. Por tanto, la red de comunicaciones que soporta estos escenarios debe respetar estrictamente esta limitación de latencia. La latencia que presenta la fibra óptica es menor de 5 ms por kilómetro de longitud.

Aunque el costo de la instalación de fibras ópticas presenta una limitación, su infraestructura de comunicación es muy rentable gracias a sus características, lo que hace de ésta una buena opción en el entorno de alta y media tensión en donde las distancias son mayores y las radiaciones electromagnéticas más intensas.

- **Medios de Cobre.**

El medio más utilizado para las comunicaciones de datos es el cableado que utiliza alambres de cobre para señalizar bits de control y de datos entre los dispositivos de red. El cableado utilizado para las comunicaciones de datos generalmente consiste en una secuencia de alambres individuales de cobre que forman circuitos que cumplen objetivos específicos de señalización.

Existen varios tipos de alambres de cobres aplicados a nivel de redes de comunicaciones, se detallan las funciones principales:

- ✓ Los **cables coaxiales**, tienen un conductor simple que circula por el centro del cable envuelto por el otro blindaje, pero está aislado de éste, Estos cables pueden utilizarse para conectar los nodos de una LAN a los dispositivos intermediarios, como routers o switches. Los cables también se utilizan para conectar dispositivos WAN a un proveedor de servicios de datos, como una compañía telefónica. Cada tipo de conexión y sus dispositivos complementarios incluyen requisitos de cableado estipulados por los estándares de la capa física. Los valores de voltaje y sincronización en estas señales son susceptibles a la interferencia o "ruido" que se genera fuera del sistema de comunicaciones. El diseño del cable coaxial ha sido adaptado para diferentes necesidades, se utilizan para colocar antenas en los dispositivos inalámbricos. También transportan energía de radiofrecuencia (RF) entre las antenas y el equipo de radio.
- ✓ El **cableado de par trenzado no blindado** (UTP), como se utiliza en las LAN Ethernet, consiste en cuatro pares de alambres codificados por color que han sido trenzados y cubiertos por un revestimiento de plástico flexible.

- ✓ El **cableado UTP**, con una terminación de conectores RJ-45, es un medio común basado en cobre para interconectar dispositivos de red, como computadoras, y dispositivos intermediarios, como routers y switches de red.
- ✓ El **cable STP** cubre todo el grupo de alambres dentro del cable al igual que los pares de alambres individuales. STP ofrece una mejor protección contra el ruido que el cableado UTP pero a un precio considerablemente superior.

Herramientas & Software de la asignatura

La herramienta que se utilizara en la materia de redes de computadoras son la siguiente:

- Análisis de paquetes (sniffer) se utilizará wireshark que puede ser descargada desde su sitio web https://www.wireshark.org/download.html
- Para emular, configurar, probar y solucionar problemas de redes virtuales y reales se dispone de la herramienta que pueden utilizar:
    - GNS3 que está disponible en su sitio web https://www.gns3.com/software/download-vm .
    - EVE Emulated Virtual Environment que está disponible en su sitio web https://www.eve-ng.net/index.php/download/#DL-COMM .

Bibliografía

Alejandra, R. B. (s.f.). Recuperado el 02 de 05 de 2021, de https://sites.google.com/site/605bredesdecomputadoras/

Amaya Carrión, E. W. (28 de 08 de 2018). *Repositorio digital* . Recuperado el 02 de 05 de 2021, de https://repositorio.une.edu.pe/

ANA, S. (s.f.). *El blog de Anita*. Recuperado el 02 de 05 de 2021, de https://espaxioinformativo.wordpress.com/

aselcom. (07 de 07 de 2020). *Aselcom*. Recuperado el 02 de 05 de 2021, de Electrònica y Telecomunicaciòn: https://www.aselcom.com/2020/07/07/evolucion-de-las-telecomunicaciones/

ccnadesdecero.com. (s.f.). *ccnadesdecero*, Volumen 1. Recuperado el 02 de 05 de 2021, de https://ccnadesdecero.com/curso/

CISCO. (02 de 05 de 2021). *CISCO*. Obtenido de https://www.cisco.com

cmapspublic2.ihmc.us. (s.f.). *IHMC Public Cmaps (2)* . Recuperado el 02 de 05 de 2021, de https://cmapspublic2.ihmc.us/

ecuared. (s.f.). Recuperado el 02 de 05 de 2021, de https://www.ecured.cu/Software_de_Red

Facultad de Ingenieria - Universidad de Buenos Aires. (s.f.). *Laboratorios de Comunicaciones*. Recuperado el 02 de 05 de 2021, de http://materias.fi.uba.ar/6679/

IBM. (s.f.). *IBM Documentation*, 7.2. Recuperado el 02 de 05 de 2021, de https://www.ibm.com/docs/es/aix

Innovave. (03 de 2016). *A/V- IT-SECURITY CONSULTING AND DESIGN*. Recuperado el 02 de 05 de 2021, de http://innovave.com/wp-content/uploads/2016/03/tia-569-c.pdf

IONOS. (18 de 07 de 2019). *Digital Guide IONOS*. Obtenido de https://www.ionos.es/digitalguide/servidores/

Ivan, G. (23 de 04 de 2015). *sites.google.com*. Obtenido de https://sites.google.com/site/cursoccna22015/

Medina, C. &. (09 de 08 de 2016). *Portal de Revistas Académicas (Investigación, Académica, Cultural, Congresos Nacionales e internacionales) de la Universidad Tecnológica de Panamá (UTP)*. Recuperado el 02 de 05 de 2021, de https://revistas.utp.ac.pa/index.php/prisma/article/view/520/

Mejía Fajardo, Á. M. (11 de 2004). *Dialnet*. Recuperado el 02 de 05 de 2021, de Ángela Marcela Mejía Fajardo

Network Startup Resource Center. (10 de 11 de 2008). *Network Startup Resource Center*. (W. p. (WALC), Productor) Recuperado el 02 de 05 de 2021, de https://nsrc.org/workshops/2008/walc/

readthedocs.io. (2017). *Planificacion administracion Redes*. Recuperado el 02 de 05 de 2021, de https://planificacionadministracionredes.readthedocs.io

Saby, R. G. (s.f.). Recuperado el 02 de 05 de 2021

sewan. (13 de 07 de 2018). Recuperado el 02 de 05 de 2021, de https://www.sewan.es/evolucion-de-las-telecomunicaciones

Sulca, M. I. (2018). *Universidad Complutense Madrid*. Recuperado el 02 de 05 de 2021, de https://informatica.ucm.es/data/cont/media/www/pag-103596/transparencias/redes-por-software-SDN.pdf

Uniòn Internacional de Telecomunicaciones. (2009). Recuperado el 02 de 05 de 2021, de https://www.itu.int/net/itunews/issues/2009/10/34-es.aspx

Universidad Autonoma del Etado de Hidalgo. (s.f.). *Apuntes Digitales - Redes de Computadoras*. Recuperado el 02 de 05 de 2021, de http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro35/index.html

Universidad de las Palmas de Gran Canaria. (s.f.). *ULPGC*. Recuperado el 02 de 05 de 2021, de https://www2.ulpgc.es/hege/almacen/download/27/27047/tema1.pdf

Universidad de Sevilla. (s.f.). *https://www.dte.us.es/personal/sivianes/tcomu/*. Recuperado el 02 de 05 de 2021, de https://www.dte.us.es/personal/sivianes/tcomu/MediosTransmision.pdf

Universidad de Valencia. (s.f.). *Instituto de Robótica - Departamento de Física Aplicada*. Recuperado el 02 de 05 de 2021, de Sistemas de Telecomunicacion .Tema 1:Historia de las Telecomunicaciones: https://www.uv.es/~hertz/hertz/Docencia/teoria/Historia.pdf

Veato pergandon, V. (26 de 05 de 2015). *Redes locales y globales*. Recuperado el 02 de 05 de 2021, de https://sites.google.com/site/redeslocalesyglobales/

wikipedia. (10 de 03 de 2021). *ARPANET*. Recuperado el 02 de 05 de 2021, de https://es.wikipedia.org/wiki/ARPANET

El contenido y gráficos de este compendio han sido obtenido mayoritariamente del curso CCNA de la academia de CISCO, información complementada con información de sitios web que se establecen en las referencias bibliográfica.

Índice

Tabla de contenido

Organización de la lectura para el estudiante por semana del compendio

Semanas	Paginas
Semana 5	Página 3 -40
Semana 6	Página 40 - 71
Semana 7	Página 72 – 95

Resultado de aprendizaje de la asignatura

Conocer los principios básicos, componentes, dispositivos, protocolos, estándares y demás elementos que intervienen en una red de comunicación.

REDES DE COMPUTADORAS

Unidad 2: **Capa Física y Enlace de Datos**

Resultado de aprendizaje de la unidad:

En la presente unidad se conocerán los fundamentos esenciales que se aplican en la capa física y enlace de datos, factores y condiciones que se deben considerar en las redes de comunicaciones para reducir y mitigar los diversos fenómenos (físicos, atmosféricos, ente otros) que intervienen en los medios de transmisión, identificando los mecanismos, técnicas e instrumentos normados que permitan resolver los problemas que se presenten a nivel de las dos primeras capas del modelo OSI.

Sabías que. - La capa de enlace de datos del modelo OSI se compone de dos subcapas: control de enlace lógico (LLC) y control de acceso al medio (MAC).

Bases teóricas para la comunicación de datos.

Para analizar la capa física en la presente unidad se iniciará con conceptos y definiciones de terminologías que se generan a nivel de esta capa.

La información es emitida por un medio de trasmisión, acción que se logra conseguir al generar en ellos una variación de sus propiedades físicas, como la tensión o la corriente que circula por él. Al representar el valor de dicha propiedad en función del tiempo, podremos modelar el comportamiento de la señal y analizarla.

Sistema de transmisión.

Un sistema de comunicación/trasmisión de datos es los encargados de transmitir un mensaje en el tiempo y espacio desde una fuente a un destinatario a través de una canal.

Señales

Una señal cualquiera viene definido por las siguientes características:

- Su **amplitud** (**A**), que es el valor máximo de la señal en un intervalo;
- Su **periodo** (**T**), que determina el intervalo de tiempo en que la señal se repite;
- Su **frecuencia** (**f**), que es el número de veces de la señal se repite en un segundo; y
- Su **fase** (**Φ**), que indica el intervalo de tiempo que va desde el instante inicial al primer punto donde la señal toma el valor 0.

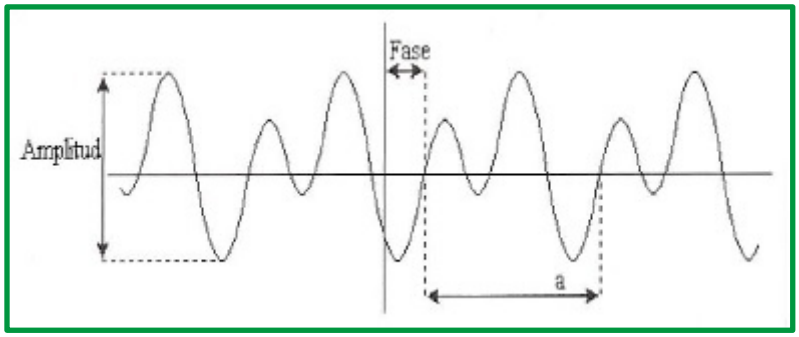


Figure 1. Características de las señales

La frecuencia se mide en hercios (Hz) y es el inverso del periodo, f=1/T. Existen dos parámetros que definen una señal, el ancho de banda y el espectro de frecuencia.

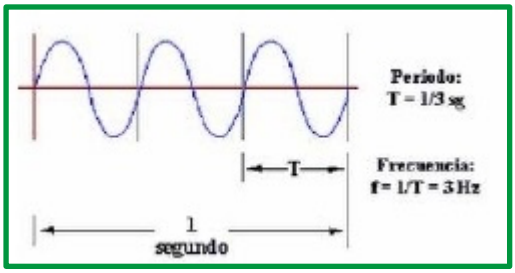


Figure 2. Parámetros de una señal

Ancho de banda.

Es el margen de frecuencias que un medio de transmisión puede soportar (gama de frecuencias por la que se transmite la señal), es la diferencia entre las frecuencias máxima y mínima que el canal es capaz de transmitir.

Ancho de banda = frecuencia máxima – frecuencia mínima

Ej.: el oído humano tiene un ancho de banda de 19.980 Hz porque puede captar sonidos entre 20 y 20.000 Hz.

Espectro

El espectro es el conjunto de frecuencias que constituyen la señal

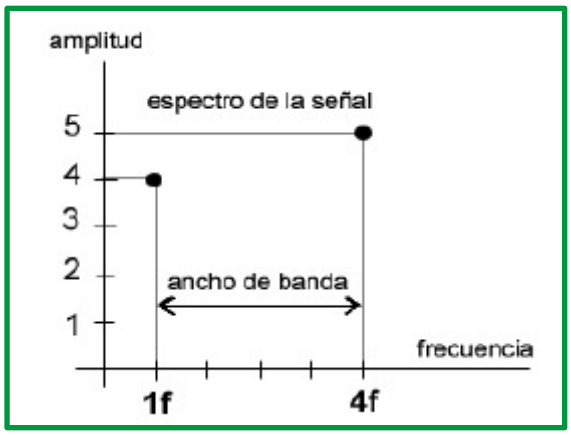


Figure 3: Espectro de señal

Distorsiones de las señales

Las distorsiones en las señales se generan en los medios de transmisiones guiados y no guiados debido a diferentes factores o fenómenos físicos, así como elementos atmosféricos que afectan a los mensajes e información no lleguen a su destino de forma íntegra. Para reducir su impacto en las comunicaciones se utilizan técnicas y mecanismo que reducen su efecto.

Entre las distorsiones de las señales tenemos:

- **Atenuación**

  Es la perdida de potencia de la señal a medida que la misma avanza en el medio de transmisión, es decir, la atenuación es el efecto producido por el debilitamiento de la señal, debido a la resistencia eléctrica que presenta tanto el canal como los demás elementos que intervienen en la transmisión, la atenuación se mide generalmente en unidades de decibelios por la longitud de unidad del medio (dB/cm, dB/km, etc) y es representado por la atenuación coeficiente del medio. Los factores de que intervienen en la atenuación son la dispersión y la absorción.

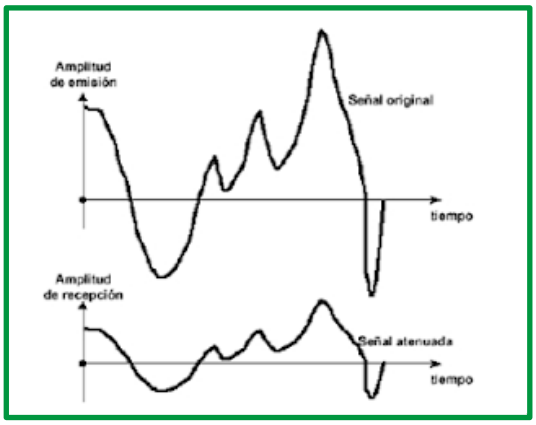


Figure 4: Atenuación de señal

- **Distorsión**

  La distorsión consiste en la deformación de la señal, producida normalmente porque el canal se comporta de modo distinto en cada frecuencia.

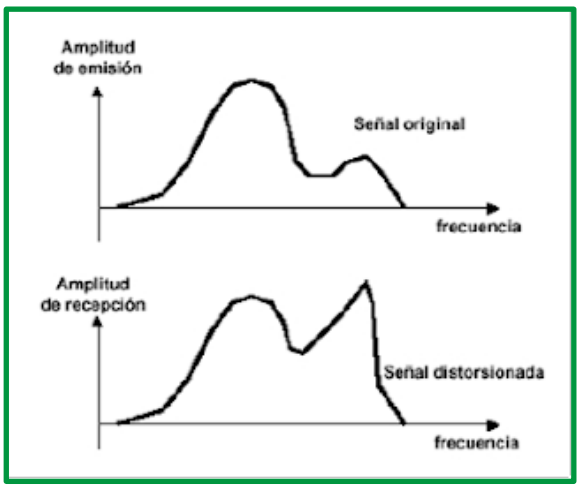


Figure 5: Distorsión de señal

- **Ruido e Interferencia**

La interferencia es causada por señales de otros sistemas de comunicación que son captadas conjuntamente a la señal propia.

Por ruido, se entiende a todo componente de tensión o intensidad indeseada que se superpone con la componente de señal que se procesa o que interfiere con el proceso de medida. El ruido se clasifica en interno o inherente y en externo o interferencias.

- ✓ **Ruido interno o inherente**: que corresponden al que se genera en los dispositivos electrónicos como consecuencia de su naturaleza física.
- ✓ **Ruido externo o interferencias**: que corresponde al que se genera en un punto del sistema como consecuencia de acoplamiento eléctrico o magnético con otro punto del propio sistema, otros sistemas naturales (tormentas, etc.) o construidos por el hombre (motores, equipos, etc.).

El ruido de interferencia puede ser periódico, intermitente, o aleatorio, se reduce, minimizando el acoplo eléctrico o electromagnético a través de blindajes o con la reorientación adecuada de los diferentes componentes y conexiones.

El ruido influye poco en los datos analógicos (por ejemplo, en una conversación telefónica) pero tiene gran importancia en los datos digitales. Hay diferentes tipos de ruido:

Ruido térmico (Ruido blanco): Este tipo de ruido es causado por la agitación térmica de los electrones dentro del conductor (varía con la temperatura). No se puede eliminar y limita las prestaciones de los sistemas de comunicación.

Ruido de intermodulación: Ocurre cuando señales de distintas frecuencias comparten el mismo medio de transmisión. Aparecen señales que son suma o resta de frecuencias. Se produce debido al funcionamiento incorrecto de los sistemas o por usar excesiva energía en la señal.

Diafonía: Se produce debido a un acoplamiento entre las distintas líneas que transportan las señales.

Ruidos impulsivos: Este ruido no es continuo, y está constituido por pulsos o picos de corta duración y gran amplitud. Puede producirse por tormentas eléctricas o fallos en los sistemas.

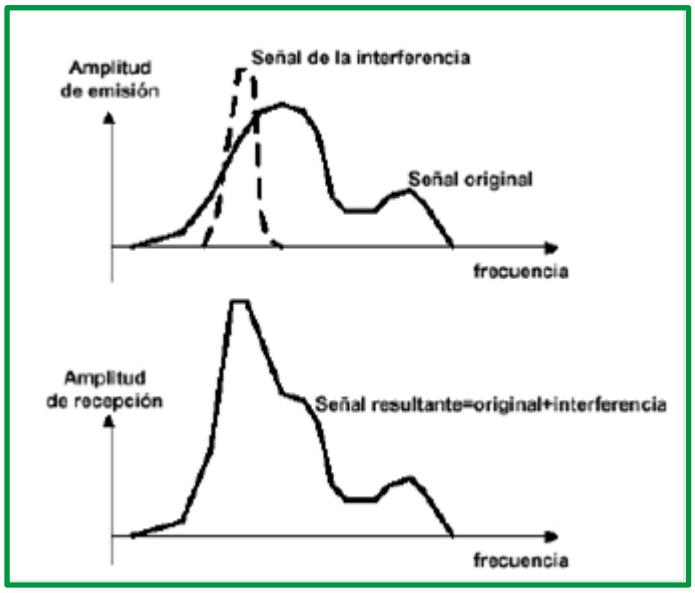


Figure 6:Interferencia de señales

Transmisión de datos

La transmisión atendiendo el tiempo de emisión se clasifican en transmisión asíncrona y transmisión síncrona.

- **Transmisión asíncrona**. Una transmisión es asíncrona cuando el proceso de sincronización entre el emisor y el receptor se realiza para cada carácter transmitido. Esto se lleva a cabo a través de unos bits especiales que ayudan a definir el entorno de cada carácter.

  Ejemplo: La línea está en reposo en el nivel lógico "1". Para avisar al receptor de que va a llegar un carácter, se antepone un bit de arranque "bit start"; con el valor lógico "0". Cuando este bit llegue al receptor, éste disparará su reloj interno y esperará por los sucesivos bits que contendrán la información del carácter transmitido. Al final se establecerá el bit de parada "bit top" que corresponderá al "1" y restaurará la línea.

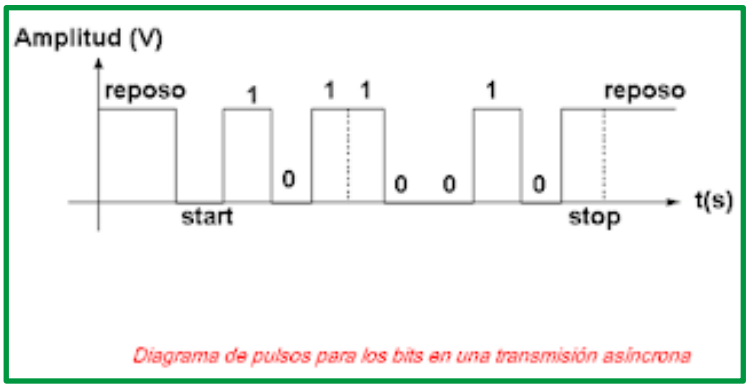


Figure 7: Proceso de transmisión asíncrona

- **Transmisión síncrona**. La transmisión es síncrona cuando se transmite un bloque de bits sin utilizar caracteres de principio y final: los bits se envían con una frecuencia constante. El emisor y el receptor se encargan de la sincronización de modo que sean capaces de reconstruir la información original. Esto exige que los dos extremos de la comunicación sincronicen sus relojes para asegurar una duración del bit constante e igual en ambos extremos. Esto puede hacerse, por ejemplo, enviando la señal de reloj por una línea independiente.

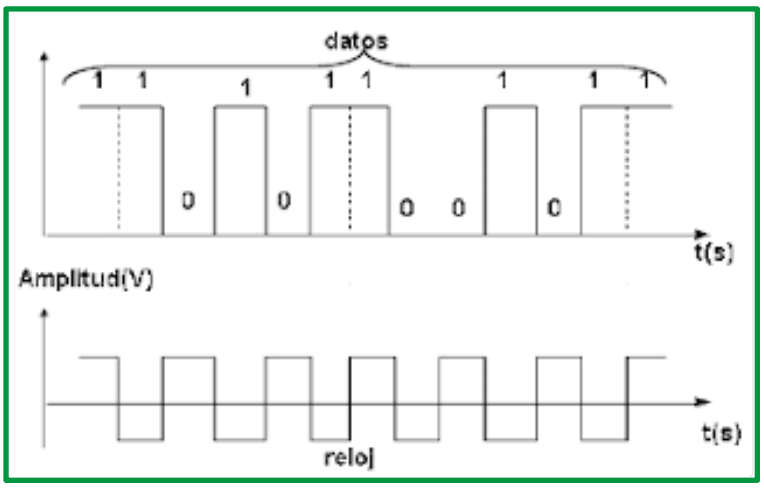


Figure 8:Proceso de transmisión síncrona

- El rendimiento de la transmisión se calcula como:
    - **Rendimiento = (bits informativos / bits transmitidos) * 100**

  Para el caso de la transmisión asíncrona, se envía 1 bit de **start** + 8 bits de **carácter** + 2 bits de **stop** = **11 bits** transmitidos por cada carácter (un carácter son 8 bit de información). Por lo tanto, el rendimiento de la transmisión asíncrona es:

  Rendimiento de la transmisión asíncrona = 8 / 11 * 100 = 72,7 %

  Para el caso una transmisión síncrona donde se transmiten bloques de 1Kbyte y el protocolo de comunicaciones envía tres caracteres SYN de sincronismo cada 256 bytes, el rendimiento de la transmisión es:

  Rendimiento de la transmisión síncrona = 1024 / (1024 + 12) * 100 = 98,8 %

La transmisión, según el medio de transmisión que utilice se clasifican en transmisión en serie y en transmisión en paralelo.

- **Transmisión en serie**. Todas las señales se transmiten por una única línea de datos secuencialmente. Los bits se transmiten en cadena por la línea de datos a una velocidad constante negociada por el emisor y el receptor. Esta forma de envío es más adecuada en transmisiones a largas distancias.
- **Transmisión en paralelo**: La transmisión de los datos se efectúa en paralelo cuando se transmiten simultáneamente un grupo de bits, uno por cada línea del mismo canal. Una transmisión en paralelo será n veces más rápida que su equivalente en serie, donde n es el número de líneas, sin embargo, la complejidad de un canal paralelo y los condicionamientos eléctricos hacen que exista una mayor dificultad en emplear este tipo de canales en grandes distancias; por lo que suelen utilizarse en ámbitos locales.

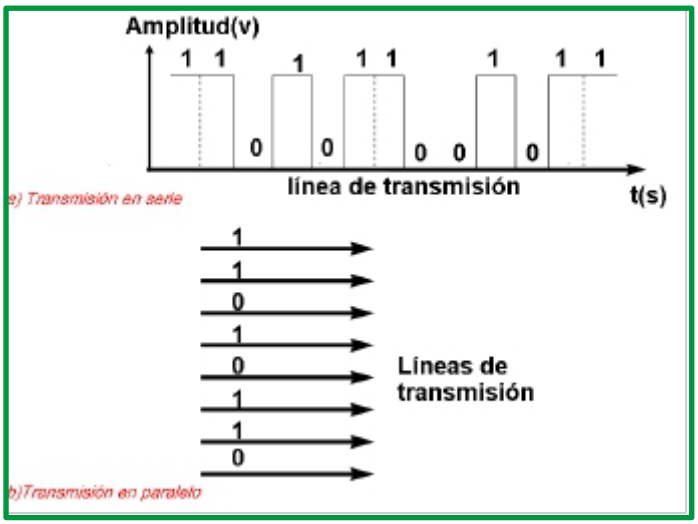


Figure 9:Transmisión en serie y paralelo

La transmisión, según la señal trasmitida se clasifican en trasmisiones analógicas y digital y transmisiones en banda base y en banda ancha.

- **Transmisión analógica y digital**. Se pueden clasificar las transmisiones en analógicas y digitales según el tipo de señal que utilicen; si es analógica, es capaz de tomar todos los valores posibles en un rango determinado y cuando las señales trasmitidas son digitales pueden tomar un número finito de valores.

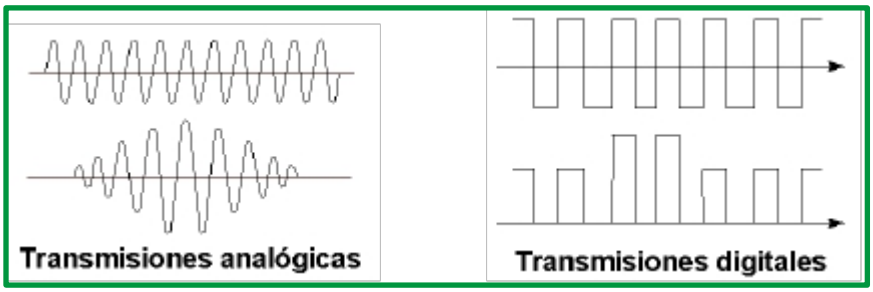


Figure 10:Transmisión análoga y digital

- **Transmisión en banda base y en banda ancha**. Los medios de transmisión en banda base establecen que solamente una señal digital puede viajar por el medio. Los medios de transmisión en banda ancha permiten que varias señales puedan viajar al mismo tiempo por el medio.

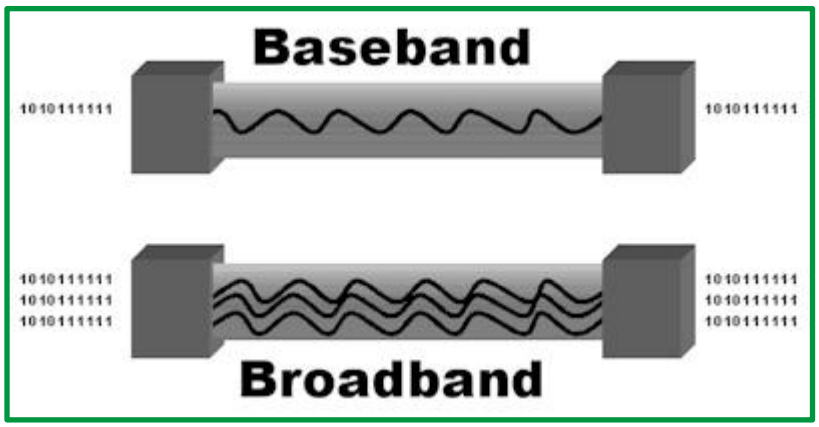


Figure 11:Transmisión en banda base y banda ancha

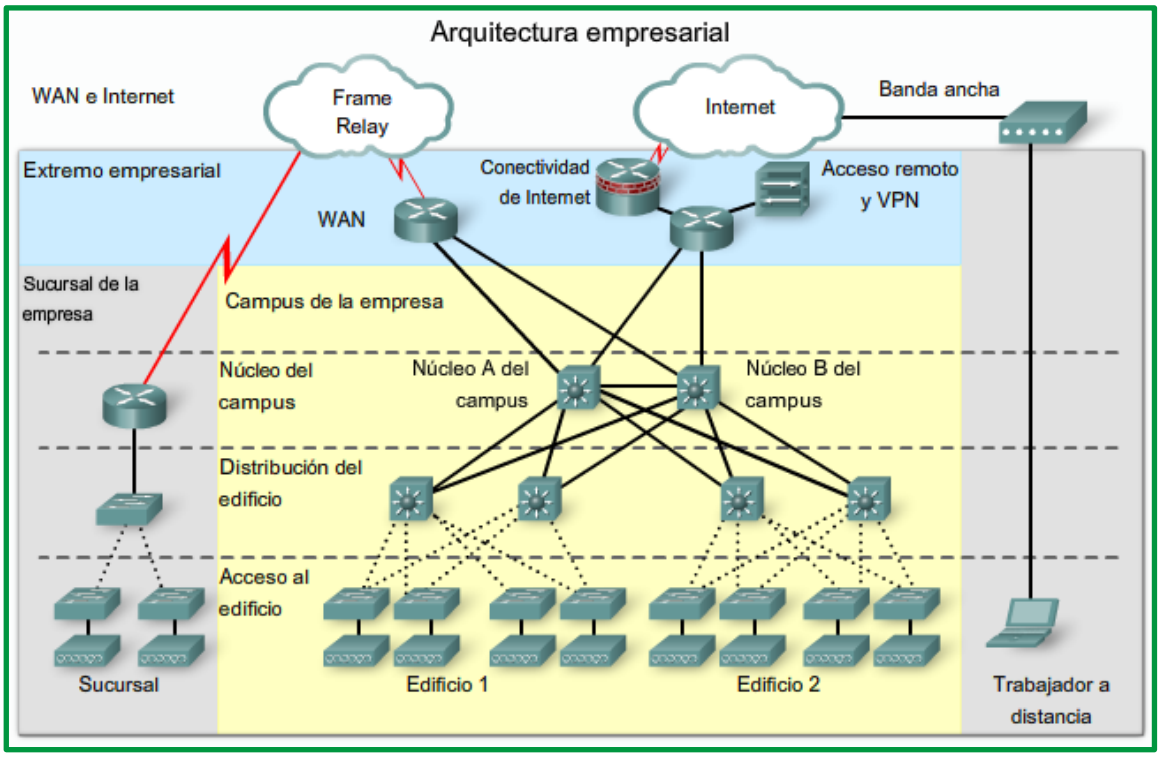


Figure 12:Ejemplo de arquitectura empresarial

Los datos que se trasmiten por los medios de comunicación pueden ser a datos análogas o datos digitales.

- **Datos análogos**: Representado por una onda electromagnética que varía continuamente con el mismo espectro que los datos.
- **Datos digitales**: Secuencia de pulsos de tensión que representan los valores binarios (0 y 1) de la señal.

Codificación.

La codificación de los datos se puede realizar usando señales unipolares donde la tensión es siempre del mismo signo (se codifica un 0 como una tensión baja y un 1 como una tensión alta (o al revés)) o señales bipolares donde la tensión toma valores positivos y negativos (se codifica un 1 como una tensión positiva y un 0 como negativa (o al revés)). A continuación, se presentan algunos de los métodos de codificación más utilizados.

- **Códigos NRZ (No retorno a cero)**. Se caracteriza por representar a cada dígito por un único nivel físico. Se codifica un nivel de tensión como un 1 y una ausencia de tensión como un 0 (o al revés). En NRZ neutral y NRZ polar se asigna, a cada dígito, un nivel de tensión diferente. En NRZ bipolar se asigna 0V para el 1 y un voltaje alterno para el 0. Esta codificación es fácil de implementar y hace un uso eficaz del ancho de banda, pero no tiene capacidad de sincronización. Esta codificación se utiliza en los estándares Ethernet 100Base-T.

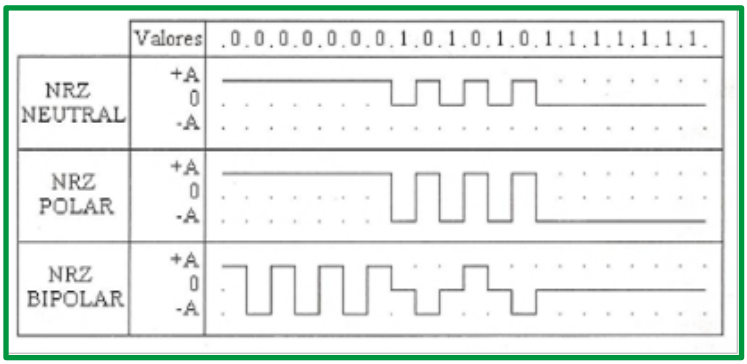


Figure 13:Códigos NRZ

- **Códigos NRZ-M (No retorno a cero modificado)**. Se caracteriza por representar a cada dígito por un cambio de nivel físico. El 0 se codifica manteniendo el nivel de la señal y el 1 cambiando de nivel. El código NRZ-M neutral tiene una amplitud entre 0 y un valor A, mientras que NRZ-M polar está entre +A y –A.

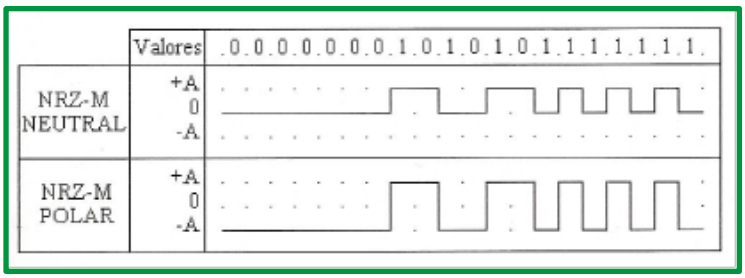


Figure 14:Códigos NRZ-M

- **Códigos RZ (Retorno a cero).** Se caracteriza por utilizar pulsos cuya amplitud es igual a la mitad del intervalo. Existe un mejor sincronismo, pero el ancho de banda del medio debe ser el doble.
    - El código RZ neutral codifica el 0 como un nivel alto +A y una transición a 0V en la mitad del Intervalo de duración del bit, mientras que para el 1 se mantiene el nivel bajo sin transición.
    - El código RZ polar representa el 0 como una transición de +A a -A en la mitad del intervalo de duración del bit. Para 1, no hay transición.
    - El código RZ bipolar codifica el 1 sin transiciones. En cambio, para el 0, utiliza niveles alternativos con transiciones a mitad del intervalo

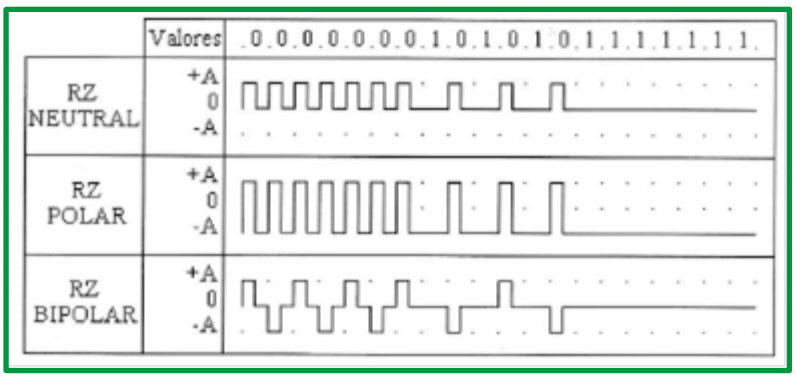


Figure 15:Códigos RZ

- **Códigos Bifase**. Se caracteriza por representar cada dígito mediante una o más transiciones. Aumenta el sincronismo, debido a que la transición ocurre durante el intervalo de duración de un bit. Pero el ancho de banda necesario es mayor.
    - **En Bifase-L** (codificación Manchester) se codifica el 0 como un flanco de bajada, mientras que el 1 es un flanco de subida. Bifase-M codifica un 0 como una transición en mitad del intervalo, mientras que el 1 no produce transición (al contrario que Bifase-S). La codificación Manchester se usa en muchos estándares de telecomunicaciones, como por ejemplo Ethernet (IEEE 802.3).

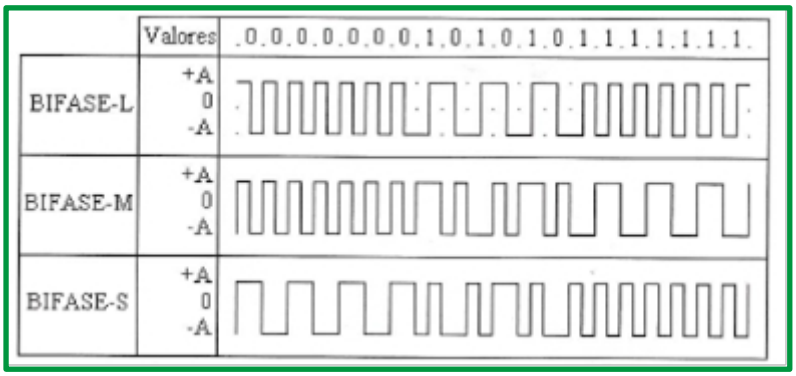


Figure 16:Código Bifase

    - En la codificación Manchester diferencial, la transición a mitad del intervalo se utiliza tan sólo para proporcionar sincronización. La transición al principio del intervalo del bit representa un 0. La ausencia de transición al principio representa un 1. Esta codificación está especificada en el estándar IEEE 802.5 para redes Token Ring.
- **Código Miller**. Se caracteriza porque un 1 produce una transición en el punto medio del intervalo y un 0 no produce una transición a no ser que vaya seguido de otro 0, en cuyo caso se produce una transición entre ambos ceros al final del primer intervalo. Las transiciones se realizan con una amplitud comprendida entre los valores +A y –A.

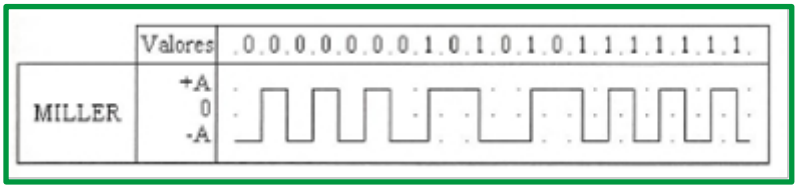


Figure 17:Código Miller

Modulación

La modulación consiste en modificar una señal continua de frecuencia constante, denominada señal portadora, para representar la información que se quiere transmitir. La modulación permite transmitir datos digitales mediante señales analógicas convirtiendo los datos a un formato analógico.

Existen varias técnicas de modulación. Todas ellas implican la modificación de uno o más de los parámetros fundamentales (amplitud, frecuencia y fase) de la señal portadora. Las técnicas básicas de modulación son:

- **Modulación por desplazamiento de amplitud (Amplitude-Shift Keying - ASK)**: Los valores binarios se representan mediante dos amplitudes diferentes de la portadora, manteniendo la frecuencia y la fase constantes. En esta técnica de modulación, es normal que una de las amplitudes sea cero; es decir, se utiliza la presencia o ausencia de la portadora. Este tipo de modulación es sensible al ruido atmosférico, distorsiones, etc. Por lo que se usa en transmisiones de hasta 1.200 bps en líneas de calidad telefónica. La modulación ASK también es usada para transmitir datos digitales sobre la fibra óptica donde el valor binario 1 es representado por un pulso corto de luz y el valor binario 0 por la ausencia de luz.
- **Modulación por desplazamiento de frecuencia (Frequency-Shift Keying - FSK):** Los valores binarios se representan por dos frecuencias próximas a la portadora, manteniendo la amplitud y la fase constantes. Este método es menos sensible a errores que la modulación por desplazamiento de amplitud ASK. Se utiliza para transmisiones de teléfono a altas frecuencias, y para LAN's con cables coaxiales.
- **Modulación por desplazamiento de fase (Phase-Shift Keying - PSK):** Este tipo de modulación se basa en el desplazamiento de la fase de la señal portadora manteniendo la amplitud y la frecuencia. Cuando hay un cambio de digito se produce un desplazamiento de la fase; por ejemplo, la mitad del periodo de la portadora. Hay diversas variantes de la modulación PSK. La modulación PSK diferencial aplica un desplazamiento en fase de (180º) y relativo a la fase correspondiente al último símbolo transmitido, en lugar de ser relativo a algún valor constante de referencia. Empleando este sistema se garantizan las transiciones o cambios de fase en cada bit, lo que facilita la sincronización del reloj del receptor. Existen varias variaciones de este tipo de modulación donde se utilizan varios ángulos de fase, haciendo posible codificar más de un bit en cada intervalo de tiempo.

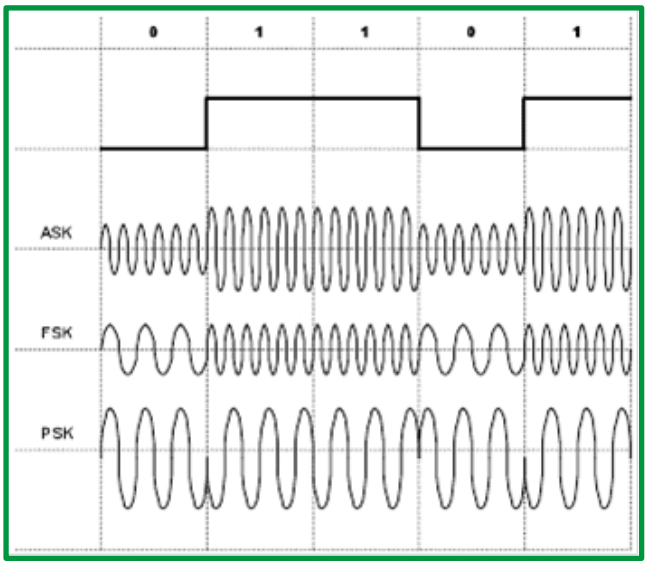


Figure 18:Modulaciones

- **Modulación PSK en cuadratura - Quadrature Phase-Shift Keying (QPSK)** Si se realizan desplazamientos de fase correspondientes a múltiplos de 1/2 (90º), habrá 4 posibles ángulos de fase y cada elemento de señal podrá representar dos bits.Utilizando 12 ángulos de fase, cuatro de los cuales tienen dos posibles amplitudes se pueden representar 24 posibilidades. Lo que hace que cada elemento de señal pueda representar 4 bits.
- **Modulación de amplitud en cuadratura - Quadrature Amplitude Modulation (QAM)** La modulación QAM consiste en modular por desplazamiento en amplitud (ASK) de forma independiente, dos señales portadoras que tienen la misma frecuencia pero que están desfasadas entre si 90º. La señal modulada QAM es el resultado de sumar ambas señales ASK. Permite codificar varios dígitos en cada intervalo de tiempo dependiendo del número de estados posibles. Se utiliza para la transmisión de datos a alta velocidad por canales con ancho de banda restringido.
- **Modulación CAP - Carrierless Amplitude and Phase Esta modulación está basada en QAM**. La diferencia fundamental radica en que la señal portadora se suprime. Es la modulación utilizada en las primeras versiones de la tecnología ADS

Multiplexación

La multiplexación es una técnica utilizada en comunicaciones mediante la cual, en un canal pueden convivir señales procedentes de distintos emisores y cuyo destino son diferentes receptores. Es decir, se comparte un canal físico, estableciendo sobre él varios canales lógicos donde intervienen dos dispositivos multiplexor y el demultiplexor.

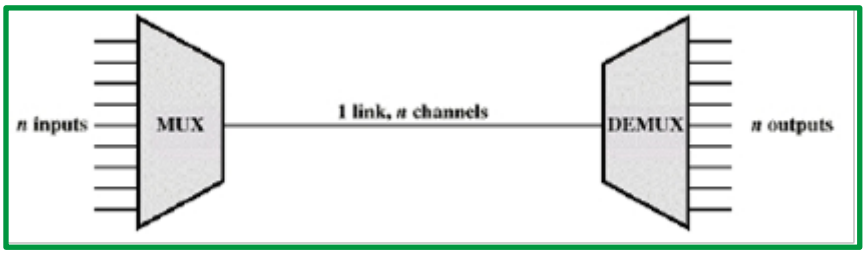


Figure 19:Técnica de multiplexación

Existen diferentes técnicas de multiplexación, se detallan las siguientes:

- **Multiplexación por división de frecuencias (FDM)**. En la multiplexación por división de frecuencias, se transmiten varias señales a través del mismo medio gracias a la asignación de una banda de frecuencias diferentes para cada canal. El ancho de banda total del canal físico se reparte entre diferentes canales lógicos. De forma que cada canal lógico tendrá un ancho de banda menor que el canal físico. Entre cada dos bandas de frecuencias consecutivas se establece una banda de seguridad para evitar las interferencias que puedan causar unos mensajes en otros. En este tipo de multiplexación, que se suele utilizar con señales analógicas, es necesario utilizar técnicas de modulación para desplazar cada señal a la banda de frecuencias asignada, y multiplexadores para combinar las señales moduladas.
- **Multiplexación por división en el tiempo (TDM).** En la multiplexación por división en el tiempo, se reparte el tiempo de uso del canal físico entre los distintos emisores estableciendo slots o ranuras temporales (intervalos de tiempo). En cada ranura de tiempo, el emisor utiliza, si lo necesita, todo el ancho de banda del canal. Cada uno de los canales utiliza el tiempo que tiene asignado, debiendo esperar a su siguiente ranura para volver a transmitir si tiene necesidad de ello. Las ranuras se repiten periódicamente con señales analógicas o digitales que transportan datos digitales. Los datos se transmiten en forma de tramas en las distintas ranuras temporales, con lo que se consigue mezclar bits de datos de varias fuentes.
- **Técnicas combinadas**. En muchas ocasiones, las comunicaciones emplean técnicas de multiplexación que combinan la multiplexación en frecuencias y en tiempo. En este tipo de multiplexación, se puede usar el canal en ciertas ranuras de tiempo. En cada ranura se transmite con un ancho de banda limitado. Las ranuras se asignan en función del grado de utilización.

Capacidad de un canal.

Es el número máximo de bits por segundo que se pueden transmitir por él. Es proporcional al ancho de banda. La capacidad de un canal depende del ancho de banda, el ruido y la tasa de errores permitida. la velocidad máxima que puede soportar un medio de transmisión determinado con respecto al tipo de señal utilizada, se emplean dos medidas: el baudio y los dígitos binarios por segundo (bps). La medida en bps indica el número de bits que se transmiten en un segundo. Por su parte, el baudio mide la cantidad de veces por segundo que la señal cambia su valor.

Análisis de Fourier

Una de las herramientas matemáticas que facilita este trabajo en el análisis de Fourier. A principios del siglo XIX, Fourier demostró que cualquier función que se comporte de forma razonablemente periódica, puede construirse mediante la suma (posiblemente infinita) de funciones seno y coseno.

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_n \, sen(2\pi nft) + \sum_{n=1}^{\infty} b_n \cos(2\pi nft)$$

Donde:

f=1/T representa la frecuencia fundamental.

a_n y b_n son las amplitudes de senos y cosenos del n-èsimo (término) armónico.

Esta descomposición se conoce como serie de Fourier.

Una señal de datos que tiene una duración finita, puede manejarse suponiendo que aquella se repite una y otra vez:

$$a_n = \frac{2}{T}\int_0^T g(t)sen(2\pi nft)dt$$

$$b_n = \frac{2}{T}\int_0^T g(t)cos(2\pi nft)dt$$

$$c = \frac{2}{T}\int_0^T g(t)dt$$

Para ver cómo aplicar la relación que existe entre el análisis de Fourier con la comunicación de datos considere el siguiente ejemplo; considérese la transmisión de carácter “b” codificado en un byte de 8 dígitos, e patrón a transmitir es 01100010.

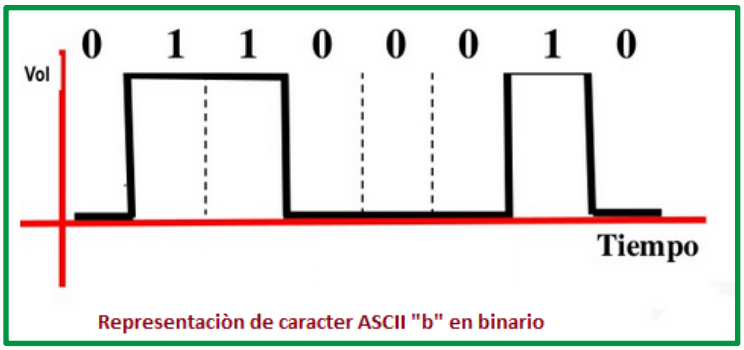


Figure 20. Representación ASCI de la letra b.

El análisis de Fourier de la señal “b” conduce a los coeficientes:

$$a_n = \frac{1}{n\pi}\left[cos\left(\frac{n\pi}{4}\right) - cos\left(\frac{3n\pi}{4}\right) + cos\left(\frac{6n\pi}{4}\right) - cos\left(\frac{7n\pi}{4}\right)\right]$$

$$b_n \frac{1}{n\pi}\left[sen\left(\frac{3n\pi}{4}\right) - sen\left(\frac{n\pi}{4}\right) + sen\left(\frac{7n\pi}{4}\right) - sen\left(\frac{6n\pi}{4}\right)\right] =$$

$$C_n = \frac{3}{8}$$

La amplitud rms de los armónicos se calcula como la energía rms=$\sqrt{a_n^2 + b_n^2}$

transmitida a cada frecuencia es proporcional al cuadrado de este valor.

En las figuras siguientes se representan los valores de los primeros términos de n.

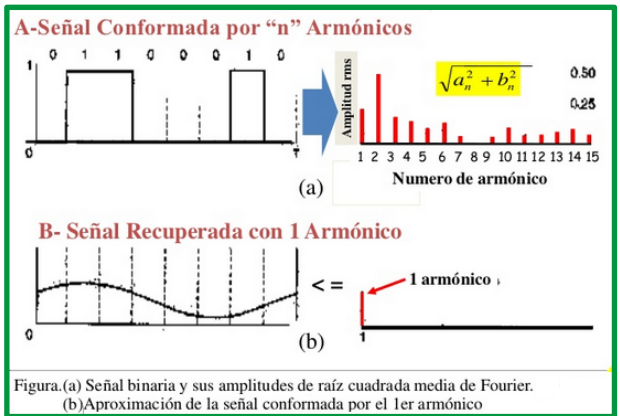


Figure 21. Señal binaria por "n" armónicos y señal recuperada con 1 armónico

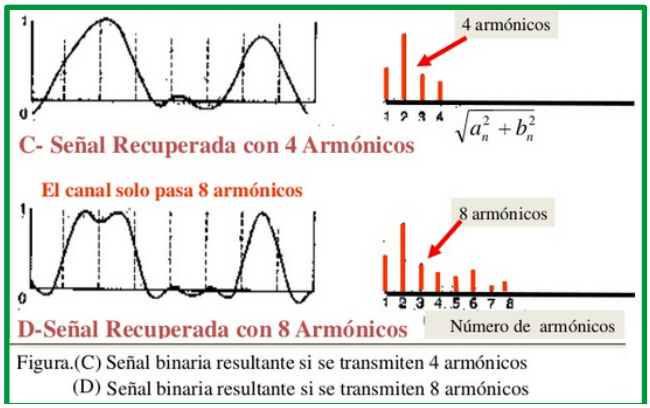


Figure 22. Señal recuperada con 4 y 8 armónicos

Al transmitir la señal, se sufre necesariamente una pérdida de potencia. Si todas las frecuencias se atenuasen por igual, la señal final sería igual a la inicial, pero con una amplitud menor. Sin embargo, esto no es así y se produce una distorsión. En general, para amplitudes desde cero hasta fc sufren una atenuación despreciable. Por encima de dicho valor, la señal es fuertemente atenuada. La posición de esta frecuencia de corte es una propiedad física del medio de transmisión.

El tiempo T que se necesita para enviar un carácter depende del método de codificación y de la velocidad de la señal (número de cambios por unidad de tiempo). El número de cambios por segundo se mide en baudios. Una línea de b baudios no transmite necesariamente b bits/s, ya que la señal puede enviar varios bits en cada nivel. Por ejemplo, si se emplean las tensiones 0,1, 2, …,7, cada nivel codifica 3 bits por lo que b baudios corresponden a 3b bps.

Si suponemos que sólo se usan dos niveles, dada una señal de b bps, el tiempo empleado para enviar 8 bits, es 8/b segundos, por lo que el primer armónico es b/8 Hz.

En una línea de calidad telefónica, la frecuencia de corte está en 3 kHz. Esto significa que el número de armónicos que pasan por ella es aproximadamente 3000/(b/8) o 24000/b.

bps	T (mseg)	Primer armónico (Hz)	nº armónicos enviados
300	26.67	37.5	80
600	13.33	75	40
1200	6.67	150	20
2400	3.33	300	10
4800	1.67	600	5
9600	0.83	1200	2
19200	0.42	2400	1
38400	0.21	4800	0

Teorema de Nyquist

En 1.924, Nyquist planteó la existencia de un límite en la capacidad de un canal ideal (sin ruido ni distorsiones) de ancho de banda finito.

Nyquist demostró que, si una señal arbitraria se hace pasar por un filtro paso bajo con un ancho de banda H, la señal filtrada puede reconstruirse por completo mediante la obtención simple y sencilla de 2H muestras por segundo. Si la señal consiste en V niveles discretos, el teorema de Nyquist establece que:

Velocidad máxima de datos (bps) = 2 H log2 (V)

Donde:

V, es el número de niveles posibles de la señal.

H, es el ancho de banda expresado en hertzios (Hz).

Este resultado es aplicable a canales sin ruido. Si existe ruido, se mide por la relación entre la potencia de la señal y la potencia del ruido, o relación señal/ruido.

En la práctica, el teorema de Nyquist significa que enviando 2H valores por segundo, como muestras de una señal de frecuencia H, podemos recomponer la señal sin perder información. Si se envían frecuencias más altas que H, serán redundantes e innecesarias para la reconstrucción de las series de valores de señal en el receptor.

En general pueden enviarse “n” bits en cualquier momento enviando 2n niveles posibles de señal. Por lo tanto, con 2n niveles de señal posibles y capaces de distinguirse, pueden transmitirse una proporción de señales de 2nH bits por segundo por un canal con un ancho de banda de H Hz.

Por ejemplo, el valor de n para una señal digital binaria es 2 por ser señales de dos niveles posibles. Un canal sin ruido de 3 kHz no podrá transmitir señales binarias a una velocidad mayor que 6.000 bps.

Teorema de Shanon

En 1.948, Shannon extendió el trabajo de Nyquist al caso de un canal real sujeto a la aparición de una cierta cantidad de ruido aleatorio. La siguiente expresión, conocida como fórmula de Shannon, proporciona la capacidad máxima en bps de un canal con ruido:

Velocidad máxima de datos (bps) = H log2 (1+S/N)

Donde:

H, es el ancho de banda del canal en Hertzios.

S, es la potencia de la señal útil, que puede estar expresada en vatios, milivatios, etc., (W, mW, etc.).

N, es la potencia del ruido presente en el canal, (mW, W, etc.) que trata de enmascarar a la señal útil. En esta fórmula se utiliza la medida de la relación señal-ruido lineal (no en dB). De esta expresión se deduce que la capacidad de los canales con poco ruido será mayor que la de aquéllos con mucho ruido.

Conmutación de paquetes y de circuitos

En las redes de comunicaciones, la forma de establecer una conexión entre dos puntos (emisor, receptor) es a través de los nodos o quipos intermedios; para establecer una conexión se requieren realizar lo siguiente:

1. **Establecimiento del circuito**.
   - ✓ El emisor solicita a un cierto nodo el establecimiento de conexión hacia una estación receptora.
   - ✓ Este nodo es el encargado de dedicar uno de sus canales lógicos a la estación emisora.
   - ✓ Este nodo es el encargado de encontrar los nodos intermedios para llegar a la estación receptora, y para ello tiene en cuenta ciertos criterios de encaminamiento, coste, etc.
2. **Transferencia de datos**.
   Una vez establecido el circuito exclusivo para esta transmisión cada nodo reserva un canal para esta transmisión, la estación, transmite desde el emisor hasta el receptor conmutando sin demoras de nodo en nodo; estos nodos tienen reservado un canal lógico para la trasmisión de datos.
3. **Desconexión del circuito.**
   Una vez terminada la transferencia, el emisor o el receptor indican a su nodo más inmediato que ha finalizado, y este nodo informa al siguiente para que se proceda con la liberación del canal establecido para la conexión; es decir de nodo en nodo se informa de la finalización para permitir la liberación del canal dedicado.

Para el establecimiento de que cada nodo pueda organizar el tráfico y las conmutaciones se aplican:

- **Conmutación de circuitos.**

  Las redes de conmutación de circuitos son las que establecen un circuito (o canal) dedicado entre los nodos y las terminales antes de que los usuarios puedan comunicarse.

  En la conmutación de circuitos, el camino (llamado "circuito") entre los extremos del proceso de comunicación se mantiene de forma permanente mientras dura la comunicación, de forma que es posible mantener un flujo continuo de información entre dichos extremos. Un ejemplo es el caso de la telefonía convencional.

  Varias conversaciones comparten la ruta interna que sigue el circuito entre los intercambios. La multiplexación por división temporal (TDM, Time Division Multiplexing) asigna a cada conversación una parte de la conexión por turno. TDM garantiza que una conexión de capacidad fija esté disponible para el suscriptor. PSTN e ISDN son dos tipos de tecnología de conmutación de circuitos que pueden utilizarse para implementar una WAN en un contexto empresarial.

  Entre sus características tenemos:

  - ✓ Los enlaces que utilizan conmutación por circuito presentan un retraso en el inicio de la comunicación. Se necesita un tiempo para realizar la conexión, lo que conlleva un retraso en la transmisión de la información, además existe un acaparamiento de recursos debido al no aprovechamiento del circuito en los instantes de tiempo en que no hay transmisión entre las partes. Se desperdicia ancho de banda mientras las partes no están comunicándose.
  - ✓ Una vez establecida la ruta de comunicación, el circuito no cambia por lo que es imposible reajustar la ruta de comunicación en cada momento para lograr el menor costo entre los nodos, es decir, una vez que se ha establecido el circuito, no se aprovechan los posibles caminos alternativos con menor coste que puedan surgir durante la sesión.
  - ✓ En la conmutación de circuitos la transmisión no se realiza en tiempo real, siendo adecuado para comunicación de voz y video, en la misma los nodos que intervienen en la comunicación disponen en exclusiva del circuito establecido mientras dura la sesión, no hay contención, una vez que se ha establecido el circuito las partes pueden comunicarse a la máxima velocidad que permita el medio, sin compartir el ancho de banda ni el tiempo de uso.
  - ✓ El circuito es fijo, una vez establecido el circuito no hay pérdidas de tiempo calculando y tomando decisiones de encaminamiento en los nodos intermedios. Cada nodo intermedio tiene una sola ruta para los paquetes entrantes y salientes que pertenecen a una sesión específica, este tipo de conmutación simplifica la gestión de los nodos intermedios una vez que se ha establecido el circuito físico,

no hay que tomar más decisiones para encaminar los datos entre el origen y el destino.

- ✓ Uno de los peores inconvenientes de la conmutación de circuito es la poca tolerancia a fallos. Si un nodo intermedio falla, todo el circuito se viene abajo. Hay que volver a establecer conexiones desde el principio.

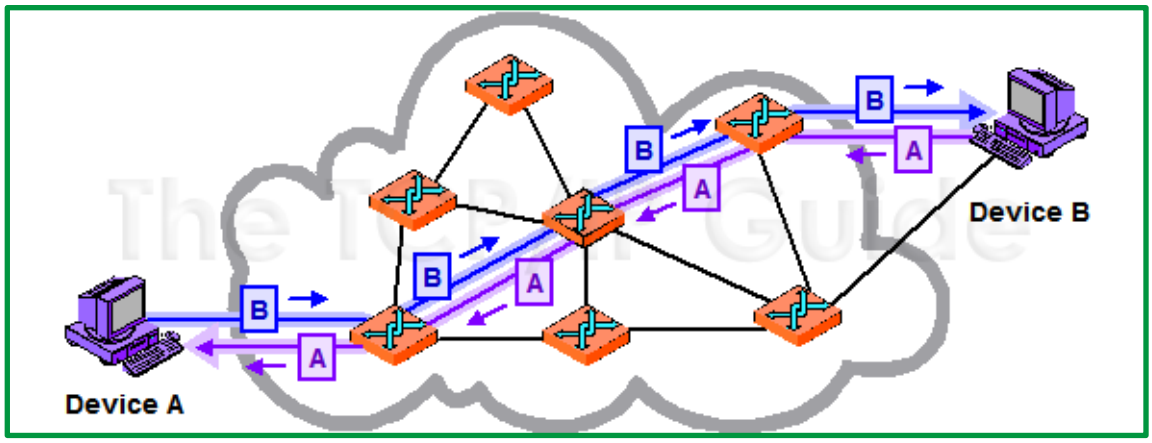


Figure 23. Conmutación de circuitos

- **Conmutación de paquetes**.

A diferencia de la conmutación de circuitos, la conmutación de paquetes divide los datos del tráfico en paquetes que se envían a través de una red compartida. Las redes de conmutación de paquetes no requieren que se establezca un circuito y permiten que muchos pares de nodos se comuniquen a través del mismo canal

La conmutación de paquetes se trata del procedimiento mediante el cual, cuando un nodo quiere enviar información a otro lo divide en paquetes, todos del mismo tamaño, los cuales contienen la dirección del nodo destino, en este caso, no existe un circuito permanente entre los extremos y, la red, simplemente, se dedica a encaminar paquete a paquete la información entre los usuarios. Entre sus características tenemos:

- ✓ Es la conmutación más usada, en caso de error en un paquete solo se reenvía ese paquete, sin afectar a los demás que llegaron sin error, se limita el tamaño de los paquetes a enviar de manera que ningún usuario pueda monopolizar una línea de transmisión durante mucho tiempo, por lo que las redes de conmutación de paquetes pueden manejar tráfico interactivo, esto hace que aumente la flexibilidad y rentabilidad de la red.
- ✓ En caso de algún fallo se puede alterar sobre la marcha el camino seguido por una comunicación así, un nodo puede seleccionar de su cola de paquetes en espera de ser transmitidos aquellos que tienen mayor prioridad.
- ✓ Los equipos de conmutación utilizados son de mayor complejidad ya que necesitan mayor velocidad y capacidad de cálculo para determinar la ruta adecuada en cada paquete, también es capaz de retrasmitir paquetes en caso de que un paquete tarde demasiado en llegar a su destino, en este caso el receptor no envía el acuse de recibo al emisor, por lo cual el receptor volverá a

retransmitir los últimos paquetes del cual no recibió el acuse, pudiendo haber redundancia de datos.

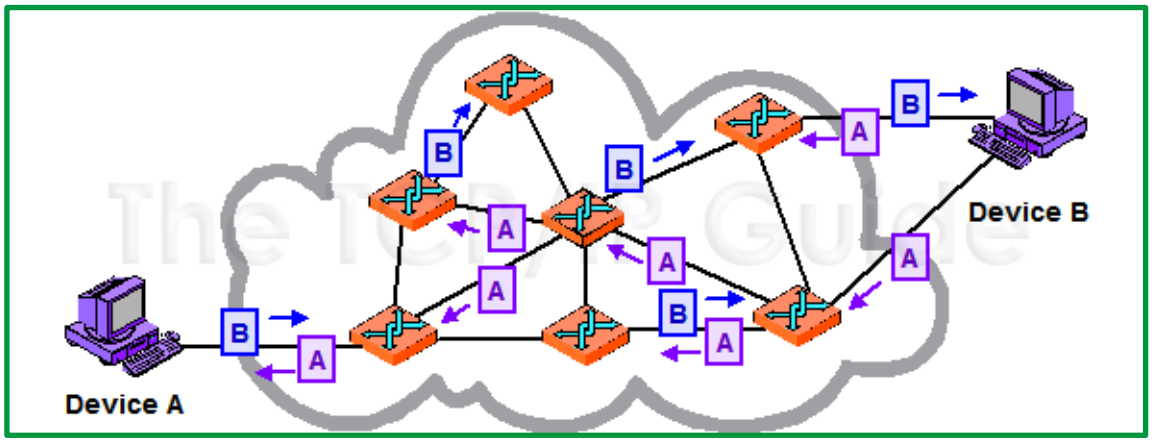


Figure 24. Conmutación por paquetes

Otra forma en la que se diferencian tecnologías y protocolos tiene que ver con si utilizan o no conexiones entre dispositivos. Este problema está estrechamente relacionado con la cuestión de la conmutación de paquetes frente a la de circuitos.

Los switches de una red conmutada por paquetes determinan el siguiente enlace por donde se debe enviar el paquete en función de la información de direccionamiento de cada paquete. Hay dos maneras de determinar este enlace: sin conexión u orientada a conexión.

- **Orientados a la conexión**.

  Un paquete es un grupo de información que consta de dos partes: los datos propiamente dichos y la información de control, que especifica la ruta a seguir a lo largo de la red hasta el destino del paquete. Existe un límite superior para el tamaño de los paquetes; si se excede, es necesario dividir el paquete en otros más pequeños. los tipos de datos que se manejan en este "medio" son: voz, datos, multimedia. (video)

  Los sistemas orientados a conexión predeterminan la ruta del paquete y cada paquete sólo necesita llevar un identificador. En el caso de Frame Relay, estos se denominan identificadores de control de enlace de datos (DLCI, Data Link Control Identifiers). El switch determina la ruta a seguir buscando el identificador en las tablas que tiene en su memoria. Este grupo de entradas en las tablas identifica una ruta o circuito particular a través del sistema. Si este circuito está físicamente disponible, sólo mientras el paquete esté pasando por él, se llama circuito virtual (VC, virtual circuit).

- **Sin conexión.**

  Transmiten toda la información de direccionamiento en cada paquete. Cada equipo (switch) debe evaluar la dirección para determinar a dónde enviar el paquete; los protocolos no establecen una conexión entre dispositivos, tan pronto como un dispositivo tiene datos para enviar a otro, simplemente los envía. Ejemplo de sistema es el internet.

Circuitos virtuales

Las redes conmutadas por paquetes pueden establecer rutas a través de los switches para realizar conexiones particulares de extremo a extremo. Estas rutas se denominan circuitos virtuales. Un VC es un circuito lógico creado dentro de una red compartida entre dos dispositivos de red. Existen dos tipos de VC.

- ✓ **Circuito virtual permanente (PVC, Permanent Virtual Circuit):** un circuito virtual establecido de forma permanente que consta de un modo (transferencia de datos). Los PVC se utilizan cuando la transferencia de datos entre dispositivos es constante. Los PVC reducen el uso del ancho de banda relacionado con el establecimiento y la terminación de los VC, pero aumentan los costos debido a la disponibilidad constante del circuito virtual. En general, los PVC, son configurados por el proveedor de servicios cuando el cliente solicita el servicio.
- ✓ **Circuito virtual conmutado (SVC, Switched Virtual Circuit):** son circuitos virtuales que se establecen dinámicamente a pedido y que se terminan cuando se completa la transmisión. La comunicación a través de un SVC consta de tres fases: establecimiento del circuito, transferencia de datos y terminación del circuito. La fase de establecimiento involucra la creación del VC entre los dispositivos origen y destino. La transferencia de datos implica la transmisión de datos entre los dispositivos a través del VC, y la fase de terminación de circuito implica la interrupción del VC entre los dispositivos origen y destino. Los SVC se utilizan en situaciones en las que la transmisión de datos entre los dispositivos es intermitente, principalmente para ahorrar costos. Los SVC liberan el circuito cuando se completa la transmisión, lo que genera menos costos de conexión que los que generan los PVC, que mantienen la disponibilidad del circuito virtual de manera constante.

  Para conectarse a una red de conmutación de paquetes, el suscriptor necesita un bucle local a la ubicación más cercana donde el proveedor ofrece el servicio. Esto se llama punto de presencia (POP, point-of-presence) del servicio. Por lo general, se trata de una línea arrendada dedicada. Esta línea es mucho más corta que una línea arrendada conectada directamente a las diferentes ubicaciones del suscriptor y muchas veces transporta VC. Como es poco probable que todos los VC enfrenten la máxima demanda al mismo tiempo, la capacidad de la línea arrendada puede ser menor a la de la suma de los VC individuales. Los siguientes son ejemplos de conexiones de conmutación de paquetes o celdas:

  - ✓ X.25
  - ✓ Frame Relay
  - ✓ ATM
  - ✓ MPLS

  En la actualidad, existen muchas opciones para implementar soluciones WAN. Ellas difieren en tecnología, velocidad y costo. Estar familiarizado con estas tecnologías es una parte importante del diseño y evaluación de la red.

Terminología de la capa física de la WAN

Una de las diferencias primordiales entre una WAN y una LAN es que una empresa u organización debe suscribirse a un proveedor de servicio WAN externo para utilizar los servicios de red de una portadora WAN. Una WAN utiliza enlaces de datos suministrados por los servicios de una operadora para acceder a Internet y conectar los sitios de una organización entre sí, con sitios de otras organizaciones, con servicios externos y con usuarios remotos. La capa física de acceso a la WAN describe la conexión física entre la red de la empresa y la red del proveedor de servicios.

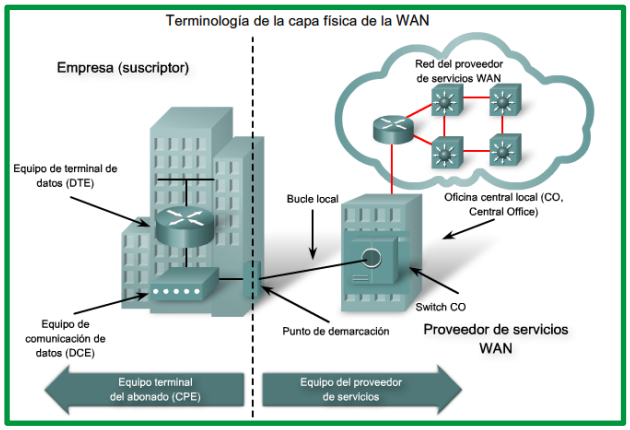


Figure 25:Conexión física entre la red de la empresa y la red del proveedor de servicios

Equipo local del cliente (CPE, Customer Premises Equipment): dispositivos y cableado interno localizados en las instalaciones del suscriptor y conectados con un canal de telecomunicaciones de una portadora. El suscriptor es dueño de un CPE o le alquila un CPE al proveedor de servicios. En este contexto, un suscriptor es una empresa que contrata los servicios WAN de un proveedor de servicios u operadora.

Equipo de comunicación de datos (DCE, Data Communications Equipment): también llamado equipo de terminación de circuito de datos, el DCE está compuesto por dispositivos que ponen datos en el bucle local. La tarea principal del DCE es suministrar una interfaz para conectar suscriptores a un enlace de comunicación en la nube WAN.

Equipo terminal de datos (DTE, Data Terminal Equipment): dispositivos del cliente que pasan los datos de la red o la computadora host de un cliente para transmisión a través de la WAN. El DTE se conecta al bucle local a través del DCE.

Punto de demarcación: punto establecido en un edificio o un complejo para separar los equipos del cliente de los equipos del proveedor de servicios. Físicamente, el punto de demarcación es la caja de empalme del cableado que se encuentra en las instalaciones del cliente y que conecta los cables del CPE con el bucle local. Normalmente se coloca en un lugar de fácil acceso para los técnicos. El punto de demarcación es el lugar donde la responsabilidad de la conexión pasa del usuario al proveedor de servicios. Esto es muy

importante porque cuando surgen problemas, es necesario determinar si la resolución o la reparación son responsabilidad del usuario o del proveedor de servicios.

Bucle local: Cable telefónico de cobre o fibra que conecta el CPE del sitio del suscriptor a la CO del proveedor de servicios. El bucle local a veces se denomina "***última milla***".

Oficina central (CO, Central Office): instalaciones o edificio del proveedor de servicios local en donde los cables telefónicos se enlazan con las líneas de comunicación de fibra óptica de largo alcance y completamente digitales a través de un sistema de switches y otros equipos.

Estándares de la capa física de una WAN.

Los protocolos de la capa física de las WAN describen cómo proporcionar conexiones eléctricas, mecánicas, operativas y funcionales para los servicios WAN. La capa física de la WAN también describe la interfaz entre el DTE y el DCE. La interfaz DTE/DCE utiliza diversos protocolos de capa física, entre ellos:

EIA/TIA-232: este protocolo permite velocidades de señal de hasta 64 Kbps en un conector D de 25 pins en distancias cortas. Antiguamente denominado RS-232. La especificación ITU-T V.24 es en efecto lo mismo.

EIA/TIA-449/530: este protocolo es una versión más rápida (hasta 2 Mbps) del EIA/TIA-232. Utiliza un conector D de 36 pins y admite cables más largos. Existen varias versiones. Este estándar también se conoce como RS-422 y RS-423.

EIA/TIA-612/613: este estándar describe el protocolo de interfaz serial de alta velocidad (HSSI, High-Speed Serial Interface), que brinda acceso a servicios de hasta 52 Mbps en un conector D de 60 pins.

V.35: este es el estándar de ITU-T para comunicaciones síncronas entre un dispositivo de acceso a la red y una red de paquetes. Originalmente especificado para soportar velocidades de datos de 48 kbps, en la actualidad soporta velocidades de hasta 2.048 Mbps con un conector rectangular de 34 pins.

X.21: este protocolo es un estándar de UIT-T para comunicaciones digitales síncronas. Utiliza un conector D de 15 pins.

Estos protocolos establecen los códigos y parámetros eléctricos que los dispositivos utilizan para comunicarse entre sí. La selección del protocolo está determinada en mayor medida por el método de comunicación del proveedor de servicios.

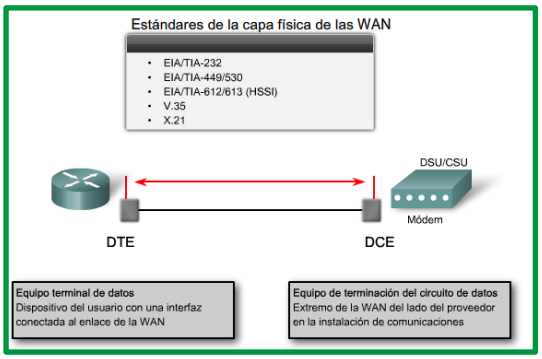


Figure 26:Estándares de la capa Física

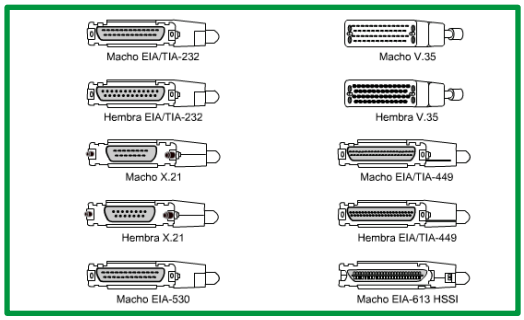


Figure 27:Conectores de cable WAN

Conmutación de tramas de datos

Las tecnologías de conmutación de tramas se basan en el uso de un dispositivo llamado conmutador o switch. Los conmutadores poseen una memoria intermedia que les permite almacenar en una cola de mensajes las tramas que llegan, lo que impide que colisionen los mensajes que reciben de forma simultánea.

Para analizar los conmutadores se procera a analizar lo siguientes elementos:

IEEE 802.3 (original) y el IEEE 802.3 revisado (Ethernet).

Las diferencias entre los estilos de tramas son mínimas. La diferencia más significativa entre el IEEE 802.3 (original) y el IEEE 802.3 revisado es el agregado de un delimitador de inicio de trama (SFD) y un pequeño cambio en el campo Tipo que incluye la Longitud, tal como se muestra en la figura.

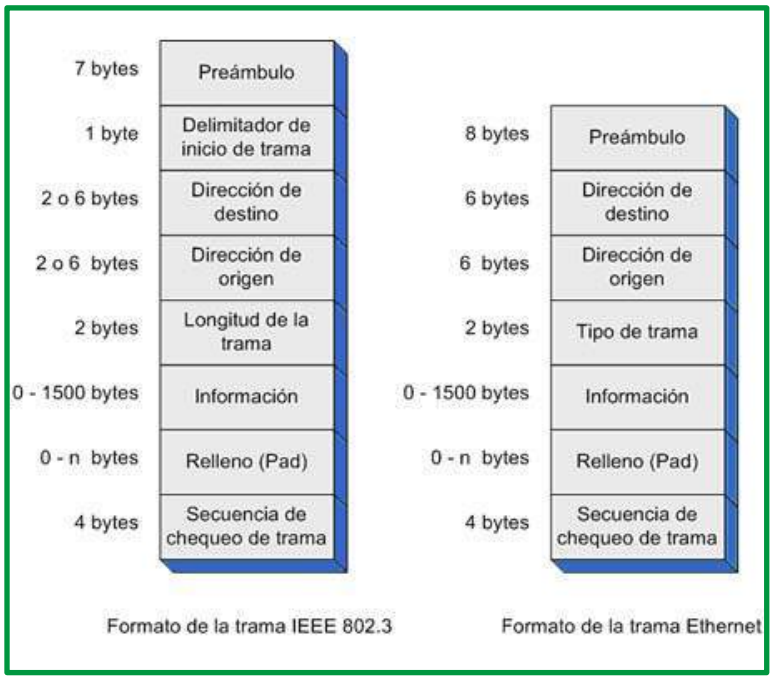


Figure 28:comparación Ethernet y 8202.3

A continuación, se describen los componentes clave del estándar Ethernet que desempeñan un importante papel en el diseño y en la implementación de las redes de conmutación.

CSMA/CD

Las señales de Ethernet se transmiten a todos los hosts que están conectados a la LAN mediante un conjunto de normas especiales que determinan cuál es la estación que puede tener acceso a la red. El conjunto de normas que utiliza Ethernet está basado en la tecnología de acceso múltiple por detección de portadora y detección de colisiones (CSMA/CD). CSMA/CD se utiliza solamente con la comunicación half-duplex que suele encontrarse en los hubs; los switches full-duplex no utilizan CSMA/CD.

Detección de portadora

En el método de acceso CSMA/CD, todos los dispositivos de red que tienen mensajes para enviar deben escuchar antes de transmitir. Si un dispositivo detecta una señal de otro dispositivo, espera un período determinado antes de intentar transmitirla. Cuando no se detecta tráfico alguno, el dispositivo transmite su mensaje. Mientras se produce dicha transmisión, el dispositivo continúa atento al tráfico o a posibles colisiones en la LAN. Una vez enviado el mensaje, el dispositivo vuelve al modo de escucha predeterminado.

Acceso múltiple

Si la distancia entre los dispositivos es tal que la latencia de las señales de un dispositivo supone la no detección de éstas por parte de un segundo dispositivo, éste también podría comenzar a transmitirlas. De este modo, los medios contarían con dos dispositivos transmitiendo señales al mismo tiempo. Los mensajes se propagan en todos los medios hasta que se encuentran. En ese momento, las señales se mezclan y los mensajes se

destruyen: se ha producido una colisión. Aunque los mensajes se dañan, la mezcla de señales continúa propagándose en todos los medios.

Detección de colisiones

Cuando un dispositivo está en el modo de escucha, puede detectar cuando se produce una colisión en los medios compartidos, ya que todos los dispositivos pueden detectar un aumento en la amplitud de la señal que esté por encima del nivel normal.

Cuando se produce una colisión, los demás dispositivos que están en el modo de escucha, además de todos los dispositivos de transmisión, detectan el aumento de amplitud de la señal. Todos los dispositivos que estén transmitiendo en ese momento lo seguirán haciendo, para garantizar que todos los dispositivos en la red puedan detectar la colisión.

Señal de congestión y postergación aleatoria

Cuando se detecta una colisión, los dispositivos de transmisión envían una señal de congestionamiento. La señal de congestionamiento avisa a los demás dispositivos acerca de la colisión para que éstos invoquen un algoritmo de postergación. La función de éste es hacer que todos los dispositivos detengan su transmisión durante un período aleatorio, con lo cual se reducen las señales de colisión.

Una vez que finaliza el retraso asignado a un dispositivo, dicho dispositivo regresa al modo "escuchar antes de transmitir". Un período de postergación aleatorio garantiza que los dispositivos involucrados en la colisión no intenten enviar tráfico nuevamente al mismo tiempo, lo que provocaría que se repita todo el proceso. Sin embargo, durante el período de postergación es posible que un tercer dispositivo transmita antes de que cualquiera de los dos involucrados en la colisión tengan oportunidad de volver a transmitir.

Trama de Ethernet

- **Campo Dirección MAC de destino**

  El campo dirección MAC de destino (6 bytes) es el identificador del receptor deseado. La capa 2 utiliza esta dirección para ayudar a que un dispositivo determine si la trama está dirigida a él. Se compara la dirección de la trama con la dirección MAC del dispositivo. Si coinciden, el dispositivo acepta la trama.

- **Campo Dirección MAC origen**

  El campo Dirección MAC de origen (6 bytes) identifica la NIC o interfaz que origina la trama. Los switches utilizan esta dirección para agregar dicha interfaz a sus tablas de búsqueda.

- **Campo Longitud/tipo**

  El campo Longitud/Tipo (2 bytes) define la longitud exacta del campo Datos de la trama. Este campo se utiliza más adelante como parte de la Secuencia de verificación de trama (FCS) con el objeto de asegurar que se haya recibido el mensaje de manera adecuada.

Aquí se puede ingresar solamente el tipo o la longitud de una trama. Si el objetivo de un campo es designar un tipo, el campo Tipo describe cuál es el protocolo que se implementa. Cuando un nodo recibe una trama y el campo Tipo/Longitud designa un tipo, el nodo determina qué protocolo de capa superior está presente. Si el valor de los dos octetos es igual o mayor que el hexadecimal de 0x0600 o decimal de 1536, el contenido del campo Datos se descifra según el protocolo indicado. Si el valor de dos bytes es menor que 0x0600, entonces el valor representa la longitud de los datos de la trama.

- **Campos Datos y Relleno**

Los campos Datos y Relleno (de 46 a 1500 bytes) contienen la información encapsulada de una capa superior, que es una PDU de Capa 3 genérica, o, más comúnmente, un paquete de IPv4. Todas las tramas deben tener una longitud mínima de 64 bytes (longitud mínima que colabora en la detección de colisiones). Si se encapsula un paquete menor, el campo Relleno se utiliza para incrementar el tamaño de la trama hasta alcanzar el tamaño mínimo.

- **Campo Secuencia de verificación de trama**

El campo FCS (4 bytes) detecta errores en una trama. Utiliza una comprobación de redundancia cíclica (CRC). El dispositivo emisor incluye los resultados de la CRC en el campo FCS de la trama. El dispositivo receptor recibe la trama y genera una CRC para buscar errores. Si los cálculos coinciden, no se ha producido ningún error. Si los cálculos no coinciden, la trama se descarta.

Tamaño de la trama de Ethernet

El estándar Ethernet original definió el tamaño mínimo de trama en 64 bytes y el tamaño máximo de trama en 1518 bytes. Esto incluye todos los bytes del campo Dirección MAC de destino a través del campo Secuencia de verificación de trama (FCS). Los campos Preámbulo y Delimitador de inicio de trama no se incluyen en la descripción del tamaño de una trama. El estándar IEEE 802.3ac, publicado en 1998, amplió el tamaño de trama máximo permitido a 1522 bytes. Se aumentó el tamaño de la trama para que se adapte a una tecnología denominada Red de área local virtual (VLAN).

Un aspecto importante a considerar es, que, si el tamaño de una trama transmitida es menor que el mínimo o mayor que el máximo, el dispositivo receptor descarta la trama. Es posible que las tramas descartadas se originen en colisiones u otras señales no deseadas y, por lo tanto, se consideran no válidas.

Comunicaciones Ethernet

Las comunicaciones en una red LAN conmutada se producen de tres maneras: unicast, broadcast y multicast.

- **Unicast**: Comunicación en la que un host envía una trama a un destino específico. En la transmisión unicast sólo existen un emisor y un receptor. La transmisión unicast es el modo de transmisión predominante en las LAN y en Internet. Una dirección MAC unicast es la dirección exclusiva que se utiliza cuando se envía una trama desde un dispositivo de transmisión único hacia un dispositivo de destino único. Algunos ejemplos de transmisiones unicast son: HTTP, SMTP, FTP y Telnet.

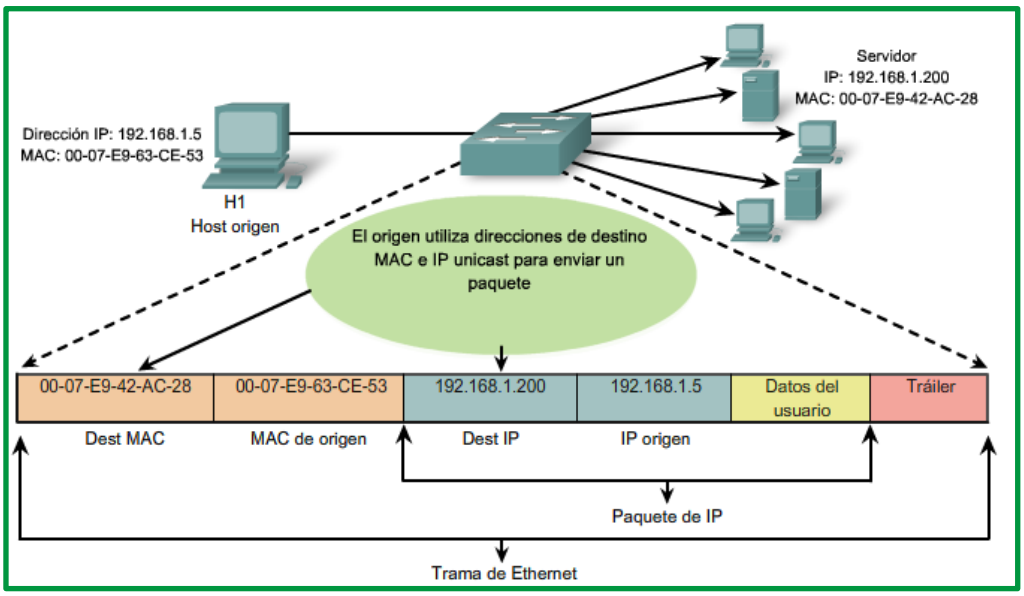


Figure 29:Dirección unicast

- **Broadcast**

  Comunicación en la que se envía una trama desde una dirección hacia todas las demás direcciones. En este caso, existe sólo un emisor, pero se envía la información a todos los receptores conectados (dominio de broadcast). La transmisión broadcast es fundamental cuando se envía el mismo mensaje a todos los dispositivos de la LAN. Un ejemplo de transmisión broadcast es la consulta de resolución de direcciones que envía el protocolo de resolución de direcciones (ARP) a todas las computadoras en una LAN.

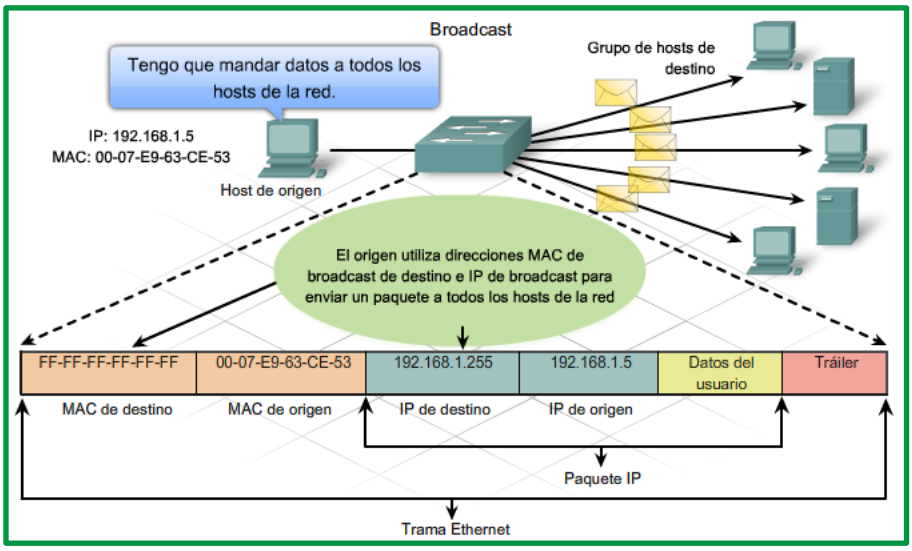


Figure 30:Dirección broadcast

Como se muestra en la figura, una dirección IP de broadcast para una red necesita una dirección MAC de broadcast correspondiente en la trama de Ethernet. En redes Ethernet, la dirección MAC de broadcast contiene 48 unos que se muestran como el hexadecimal FF-FF-FF-FF-FF-FF.

- **Multicast**
  Las direcciones multicast le permiten a un dispositivo de origen enviar un paquete a un grupo de dispositivos. Los clientes de la transmisión multicast deben ser miembros de un grupo multicast lógico para poder recibir la información.

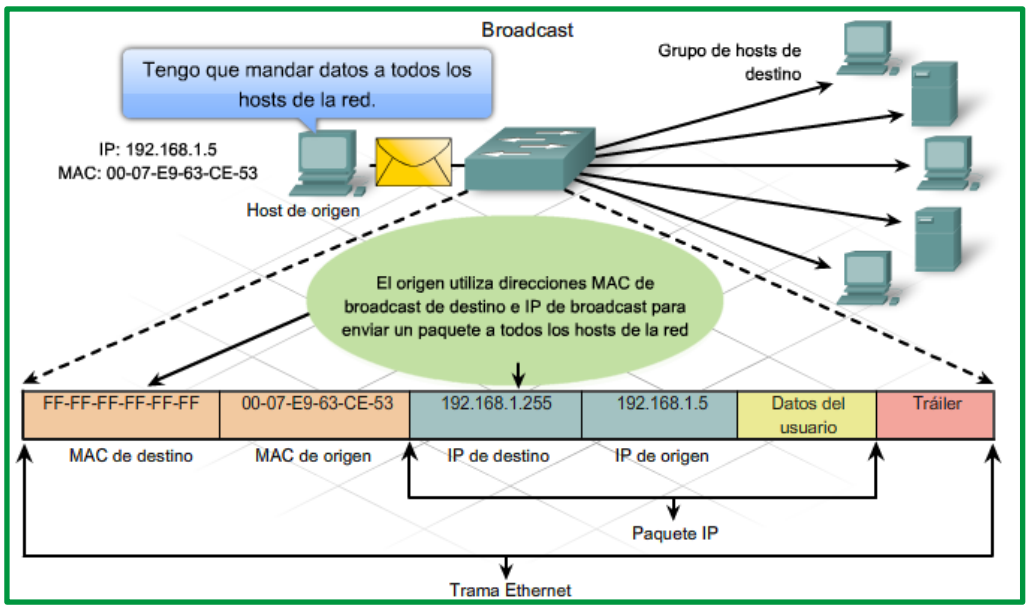


Figure 31:Dirección multicast

La dirección IP multicast requiere una dirección MAC multicast correspondiente para poder enviar tramas en una red local. La dirección MAC multicast es un valor especial que comienza con 01-00-5E en hexadecimal. El valor termina con la conversión de los

23 bits inferiores de la dirección IP del grupo multicast en los 6 caracteres hexadecimales restantes de la dirección de Ethernet. El bit restante en la dirección MAC es siempre "0".

Formato de trama de la Capa MAC

La trama de enlace de datos de capa 2 normalmente contiene información del encabezado con una **dirección de origen** y de **destino** del enlace de datos, información del tráiler y los datos reales transmitidos. La dirección de origen del enlace de datos es la dirección de Capa 2 de la interfaz que envió la trama de enlace de datos. La dirección de destino del enlace de datos es la dirección de Capa 2 de la interfaz del dispositivo de destino. Tanto la interfaz del enlace de datos de origen como la de destino se encuentran en la misma red. Cuando un paquete se envía de un router a otro, las direcciones IP de origen y destino de capa 3 no cambiarán; sin embargo, sí lo harán las direcciones de enlace de datos de origen y destino de capa 2.

La siguiente es una lista de los campos en una trama de Ethernet y una breve descripción de cada uno:

- **Preámbulo**: siete bytes que alternan 1 y 0, utilizados para sincronizar señales.
- **Delimitador de inicio de trama (SOF):** 1 byte que señala el comienzo de la trama.
- **Dirección de destino**: dirección MAC de 6 bytes del dispositivo emisor en el segmento local.
- **Dirección de origen**: dirección MAC de 6 bytes del dispositivo receptor en el segmento local.
- **Tipo/longitud**: 2 bytes que especifican ya sea el tipo de protocolo de capa superior (formato de trama de Ethernet II) o la longitud del campo de datos (formato de trama IEEE 802.3).
- **Datos y Pad**: de 46 a 1500 bytes de datos; ceros utilizados para completar cualquier paquete de datos de menos de 46 bytes.
- **Secuencia de verificación de trama (FCS):** 4 bytes utilizados para una comprobación de redundancia cíclica a fin de asegurar que no se dañó la trama.

Dirección MAC

Una dirección Ethernet MAC es un valor binario de 48 bits que se compone de dos partes y se expresa como 12 dígitos hexadecimales. Los formatos de las direcciones pueden ser similares a 00-05-9A-3C-78-00, 00:05: 9A:3C:78:00 o 0005.9A3C.7800.

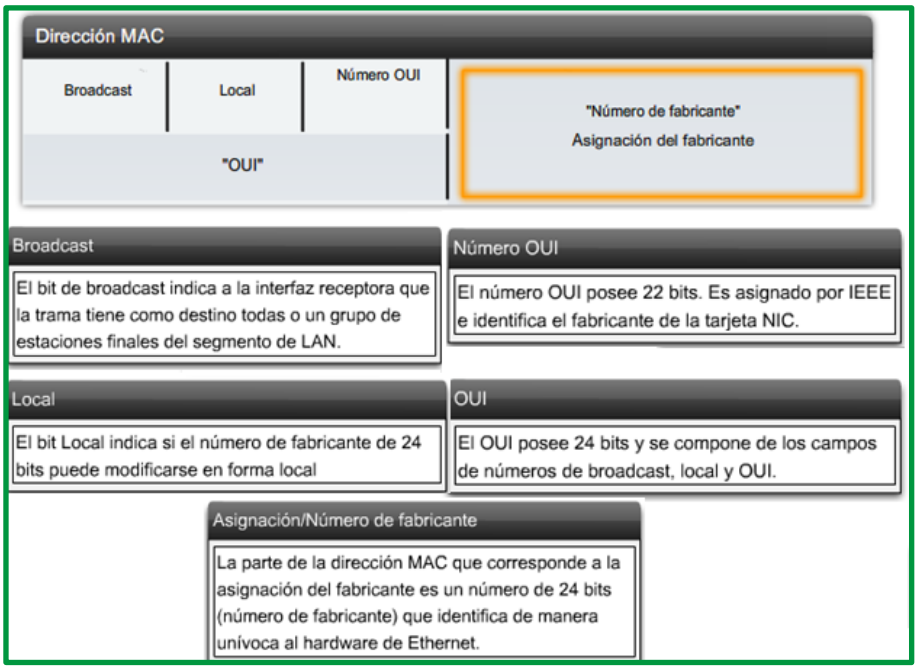


Figure 32:Descripción de dirección MAC

Todos los dispositivos conectados a una LAN Ethernet tienen interfaces con direcciones MAC. La NIC utiliza la dirección MAC para determinar si deben pasarse los mensajes a las capas superiores para su procesamiento. La dirección MAC está codificada de manera permanente dentro de un chip ROM en una NIC. Este tipo de dirección MAC se denomina dirección grabada (BIA, Burned In Address). Algunos fabricantes permiten que se modifiquen las direcciones MAC de manera local. La dirección MAC se compone del identificador exclusivo de organización (OUI) y del número de asignación del fabricante.

- **Identificador Exclusivo de Organización**

  El OUI es la primera parte de una dirección MAC. Tiene una longitud de 24 bits e identifica al fabricante de la tarjeta NIC. El estándar IEEE regula la asignación de los números de OUI. Dentro del OUI, existen 2 bits que sólo tienen significado cuando se utilizan en la dirección de destino, como se describe a continuación:

  - ✓ **Bit multicast o broadcast**: Indica a la interfaz receptora que la trama está destinada a un grupo o a todas las estaciones finales del segmento de la LAN.
  - ✓ **Bit de direcciones administrado de manera local**: Si la dirección MAC asignada por el fabricante puede modificarse en forma local, éste es el bit que debe configurarse.

- **Número de asignación del fabricante**

  La parte de la dirección MAC asignada por el fabricante es de 24 bits de longitud e identifica exclusivamente el hardware de Ethernet. Puede ser una BIA o bien con el bit modificado en forma local mediante software.

Las diferencias que existen entre Ethernet estándar, Fast Ethernet, Gigabit Ethernet y 10 Gigabit Ethernet tienen lugar en la capa física. La Ethernet se rige por los estándares IEEE 802.3.

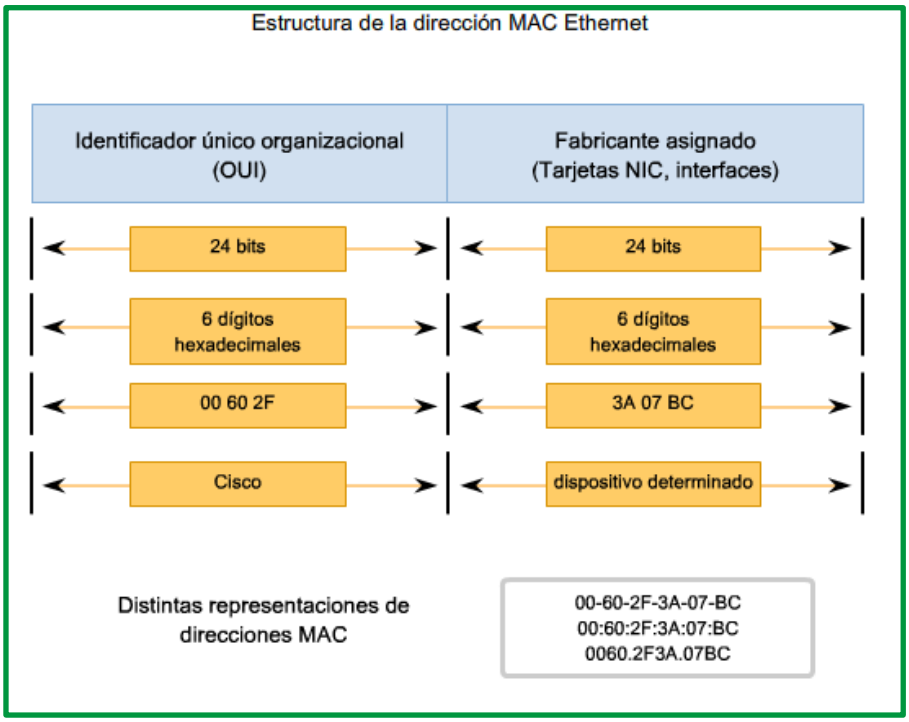


Figure 33:Estructura d la dirección MAC

Visualización de la MAC

Una herramienta útil para analizar la dirección MAC de nuestra computadora es ipconfig /all o ifconfig desde una terminal en los sistemas operativos windows y linux.

Comunicación half duplex y full duplex.

Se utilizan dos tipos de parámetros duplex para las comunicaciones en una red Ethernet: half duplex y full duplex.

Half Duplex

La comunicación half-duplex se basa en un flujo de datos unidireccional, en el que el envío y la recepción de datos no se producen al mismo tiempo. Esto es similar a la función de las radios de dos vías o dos walki-talkies, en donde una sola persona puede hablar a la vez. Si una persona habla mientras lo hace la otra, se produce una colisión. Por ello, la comunicación half-duplex implementa el CSMA/CD con el objeto de reducir las posibilidades de que se produzcan colisiones y detectarlas en caso de que se presenten. Las comunicaciones half-duplex presentan problemas de funcionamiento debido a la constante espera, ya que el flujo de datos sólo se produce en una dirección a la vez.

Las conexiones half-duplex suelen verse en los dispositivos de hardware más antiguos, como los hubs. Los nodos que están conectados a los hubs y que comparten su conexión con un

puerto de un switch deben funcionar en el modo half-duplex porque las computadoras finales tienen que tener la capacidad de detectar las colisiones. Los nodos pueden funcionar en el modo half-duplex si la tarjeta NIC no puede configurarse para hacerlo en full duplex. En este caso, el puerto del switch también adopta el modo half-duplex predeterminado. Debido a estas limitaciones, la comunicación full-duplex ha reemplazado a la half-duplex.

El rendimiento de una configuración de red compartida Ethernet estándar basada en hubs es generalmente del 50% al 60% del ancho de banda de 10 Mb/s.

Full dúplex.

En las comunicaciones full-duplex el flujo de datos es bidireccional, por lo tanto, la información puede enviarse y recibirse al mismo tiempo. La capacidad bidireccional mejora el rendimiento, dado que reduce el tiempo de espera entre las transmisiones. Actualmente, las tarjetas NIC Ethernet, Fast Ethernet y Gigabit Ethernet disponibles en el mercado proporciona capacidad full-duplex.

En el modo full-duplex, el circuito de detección de colisiones se encuentra desactivado. Las tramas enviadas por los dos nodos finales conectados no pueden colisionar, dado que éstos utilizan dos circuitos independientes en el cable de la red. Cada conexión full-duplex utiliza un solo puerto. Las conexiones full-duplex requieren un switch que admita esta modalidad o bien una conexión directa entre dos nodos compatibles con el modo full duplex. Los nodos que se conecten directamente al puerto de un switch dedicado con tarjetas NIC capaces de admitir full duplex deben conectarse a puertos de switches que estén configurados para funcionar en el modo full-duplex.

Una red Fast Ethernet full-duplex, en comparación con un ancho de banda de 10 Mb/s, ofrece un rendimiento del 100% en ambas direcciones (transmisión de 100 Mb/s y recepción de 100 Mb/s).

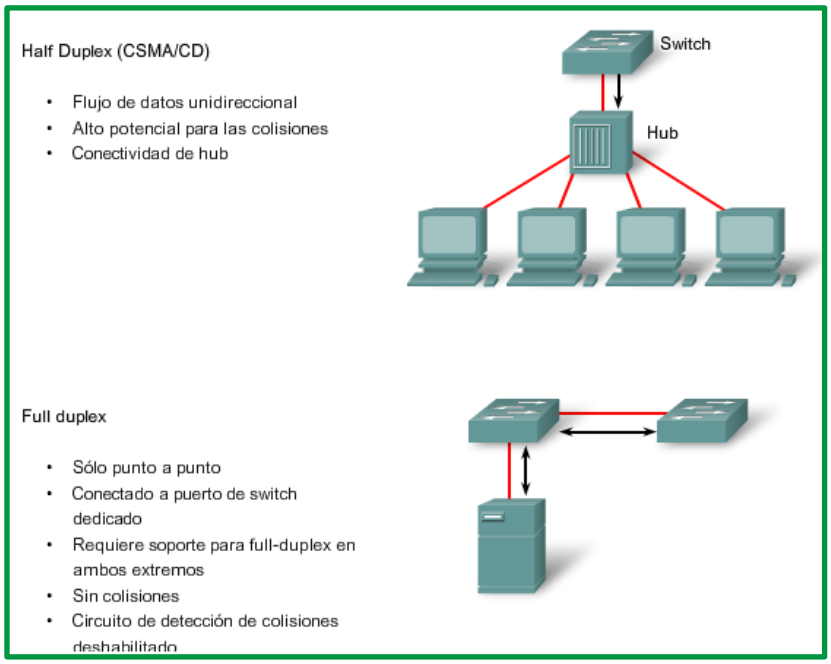


Figure 34:Communication half-duplex y full-duplex

Un elemento muy importante y que determina la capacidad de conmutación de un switch son los buffers, elementos de memoria que sirven para almacenar las tramas que van a ser reenviadas al nodo que corresponda. Los buffers realizan la función de caché, especialmente importante para conectar dos nodos con puertos a distintas velocidades, para así disminuir el efecto cuello de botella.

Existen varias técnicas de conmutación en un switch:

Almacenamiento y reenvío (Store and Forward). En este caso, cuando un switch recibe datos por un puerto, almacena la trama completa en el buffer para luego reenviarla al puerto destino. La utilización de esta técnica permite realizar algunas comprobaciones de error antes de ser enviada al puerto de destino.

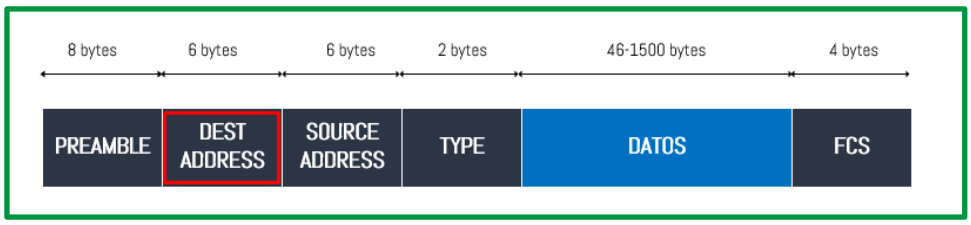


Figure 35:Trama ethernet

Mientras la trama se va recibiendo el switch va analizando la dirección de destino, este análisis de la dirección de destino, le permite al switch ir tomando decisiones sobre qué hacer con la trama, si la dirección de destino se encuentra en su tabla MAC, la trama será conmutada al puerto de salida, si la dirección de destino no se encuentra en su tabla MAC se realiza una inundación de la trama a todos sus puertos.

Algo importante a mencionar, es que la trama no va ser conmutada a otro puerto si los datos del campo FCS no son correctos. El campo FCS se utiliza para realizar la verificación de la integridad de la trama.

Reenvío directo (cut-through). En esta técnica, cuando un switch comienza a recibir datos por un puerto, no espera a leer la trama completa para reenviarla al puerto destino. En cuanto lee la dirección de destino de la trama MAC, comienza a transferir los datos al puerto destino.

El switch no espera a toda la trama para analizar qué hacer con ella, esto significa que este método no se encarga de descartar tramas cuando tengan errores de capa Física o de Enlace de datos, no se realiza la validación del campo FCS. El único dispositivo que se encarga de validar el campo FCS, es el dispositivo de destino final, si encuentra errores descarta la trama.

Esta técnica proporciona unos tiempos de retardo bastante bajos, sin embargo, tiene como inconveniente que sólo puede usarse cuando las velocidades de todos los puertos son iguales.

El método Cut-through tiene 2 versiones:

- **Fast Forward**

  Esta primera versión se encarga de conmutar la trama al puerto de salida apenas pueda leer la dirección MAC de destino. En esta versión se reduce la latencia, pero se tiene riesgos de enviar una trama con errores a través de la red.

- **Framegnt-Free**

  La segunda versión trata de enviar tramas lo más rápido posible y al mismo tiempo evita enviar tramas que tengan errores debido a colisiones. Cuando se implementó el mecanismo de acceso al medio CSMA/CD, se determinó que las colisiones que provocan errores en las tramas, deben ser detectadas en los primeros 64 bytes de la trama. Tomando en cuenta esta regla, este método espera recibir los primeros 64 bytes de la trama para recién comenzar a conmutarla al puerto de salida.

El tiempo de retardo introducido es variable ya que depende del tamaño de la trama; este método es el utilizado siempre en los switches que tienen puertos de diferente velocidad.

Direccionamiento MAC y Tablas de direcciones MAC de los switches

Los switches emplean direcciones MAC para dirigir las comunicaciones de red a través de su estructura al puerto correspondiente hasta el nodo de destino. La estructura del switch son los circuitos integrados y la programación de máquina adjunta que permite controlar las rutas de datos a través del switch. El switch debe primero saber qué nodos existen en cada uno de sus puertos para poder definir cuál será el puerto que utilizará para transmitir una trama unicast.

El switch determina cómo manejar las tramas de datos entrantes mediante una tabla de direcciones MAC. El switch genera su tabla de direcciones MAC grabando las direcciones MAC de los nodos que se encuentran conectados en cada uno de sus puertos. Una vez que la dirección MAC de un nodo específico en un puerto determinado queda registrada en la tabla de direcciones, el switch ya sabe enviar el tráfico destinado a ese nodo específico desde el puerto asignado a dicho nodo para posteriores transmisiones.

Cuando un switch recibe una trama de datos entrantes y la dirección MAC de destino no figura en la tabla, éste reenvía la trama a todos los puertos excepto al que la recibió en primer lugar. Cuando el nodo de destino responde, el switch registra la dirección MAC de éste en la tabla de direcciones del campo dirección de origen de la trama. En las redes que cuentan con varios switches interconectados, las tablas de direcciones MAC registran varias direcciones MAC para los puertos que conectan los switches que reflejan los nodos de destino. Generalmente, los puertos de los switches que se utilizan para interconectar dos switches cuentan con varias direcciones MAC registradas en la tabla de direcciones.

A continuación, se describe este proceso:

Paso 1. El switch recibe una trama de broadcast de la PC 1 en el Puerto 1.

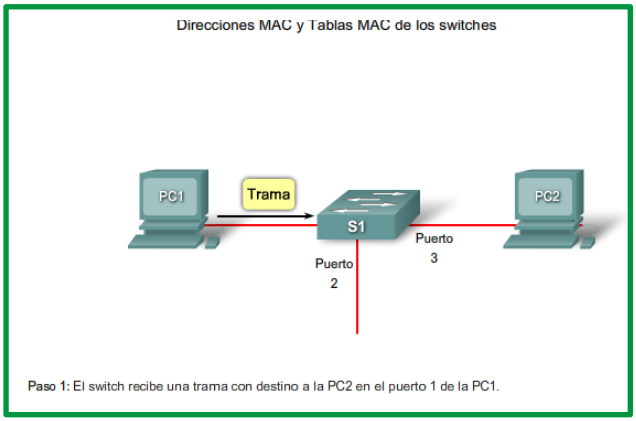


Figure 36:Proceso de actualización de la tabla de direcciones MAC.

Paso 2. El switch ingresa la dirección MAC de origen y el puerto del switch que recibió la trama en la tabla de direcciones.

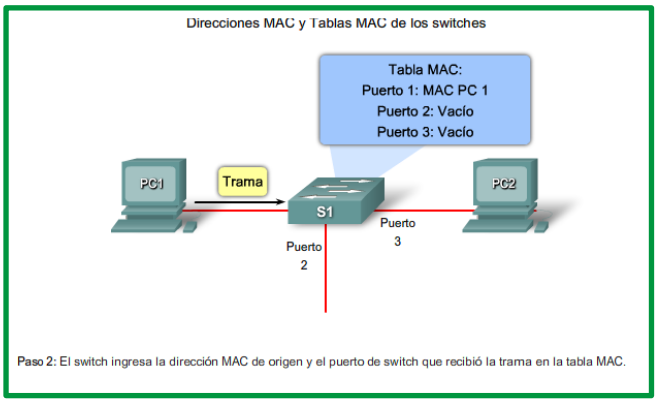


Figure 37: Proceso de actualización de la tabla de direcciones MAC.

Paso 3. Dado que la dirección de destino es broadcast, el switch genera flooding en todos los puertos enviando la trama, excepto el puerto que la recibió.

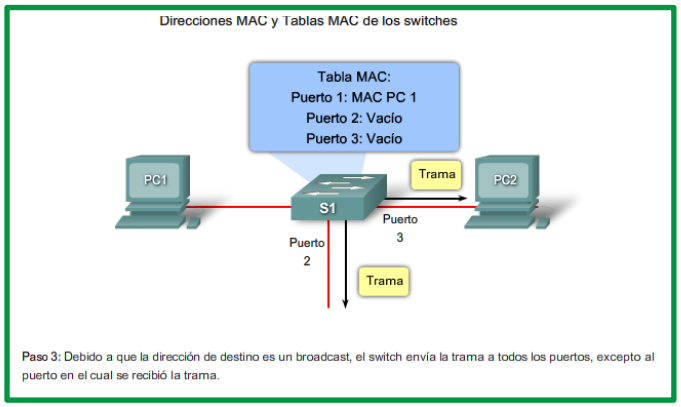


Figure 38: Proceso de actualización de la tabla de direcciones MAC.

Paso 4. El dispositivo de destino responde al broadcast con una trama de unicast dirigida a la PC 1.

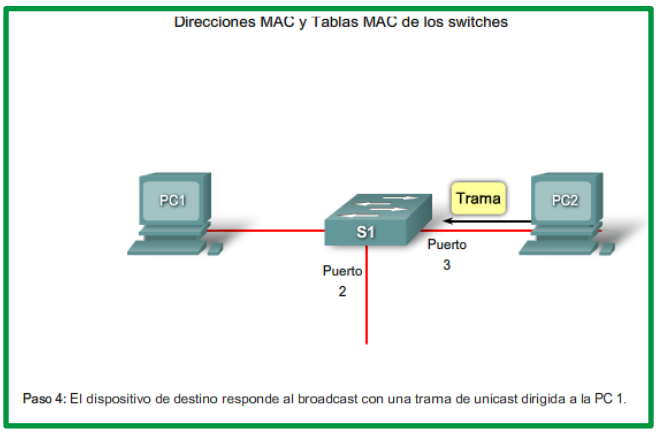


Figure 39: Proceso de actualización de la tabla de direcciones MAC.

Paso 5. El switch ingresa la dirección MAC de origen de la PC2 y el número de puerto del switch que recibió la trama en la tabla de direcciones. La dirección de destino de la trama y el puerto relacionado a ella se encuentran en la tabla de direcciones MAC.

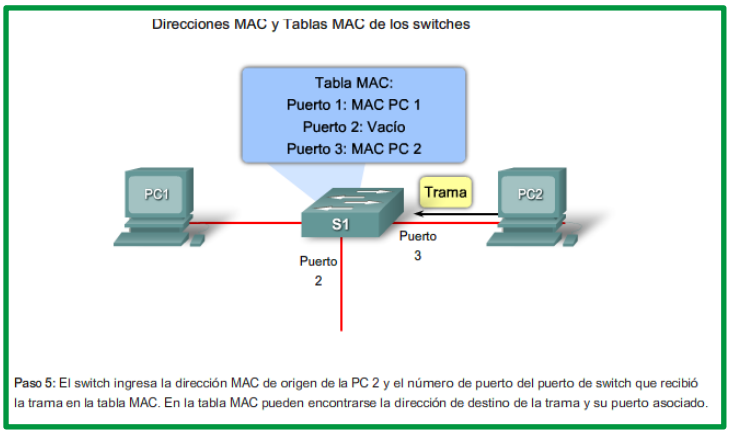


Figure 40: Proceso de actualización de la tabla de direcciones MAC.

Paso 6. Ahora el switch puede enviar tramas entre los dispositivos de origen y destino sin saturar el tráfico, ya que cuenta con entradas en la tabla de direcciones que identifican a los puertos asociados.

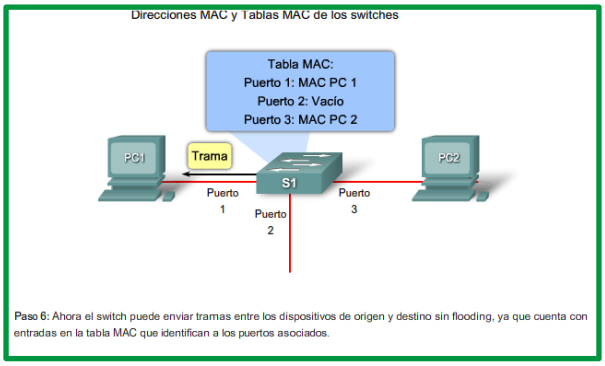


Figure 41: Proceso de actualización de la tabla de direcciones MAC.

Protocolo ARP.

El protocolo ARP ofrece dos funciones básicas:

- Resolución de direcciones IPv4 a direcciones MAC.
- Mantenimiento de una caché de las asignaciones.

Resolución de direcciones IPv4 a direcciones MAC

Para que una trama se coloque en los medios de la LAN, debe contar con una dirección MAC de destino. Cuando se envía un paquete a la capa de Enlace de datos para que se lo encapsule en una trama, el nodo consulta una tabla en su memoria para encontrar la dirección de la capa de enlace de datos que se mapea a la dirección IPv4 de destino. Esta tabla se denomina tabla ARP o caché ARP. La tabla ARP se almacena en la RAM del dispositivo.

Cada entrada o fila de la tabla ARP tiene un par de valores: ***una dirección IP*** y ***una dirección MAC***. La relación entre los dos valores se denomina mapa, que simplemente significa que usted puede localizar una dirección IP en la tabla y descubrir la dirección MAC

correspondiente. La tabla ARP almacena el mapeo de los dispositivos de la LAN local en la memoria caché.

Para comenzar el proceso, un nodo transmisor intenta localizar en la tabla ARP la dirección MAC mapeada a un destino IPv4. Si este mapa está almacenado en la tabla, el nodo utiliza la dirección MAC como la MAC de destino en la trama que encapsula el paquete IPv4. La trama se codifica entonces en los medios de la red.

Mantenimiento de una tabla ARP

La tabla ARP se mantiene dinámicamente. Existen dos maneras en las que un dispositivo puede reunir direcciones MAC. Una es monitorear el tráfico que se produce en el segmento de la red local. A medida que un nodo recibe tramas de los medios, puede registrar las direcciones IP y MAC de origen como mapeos en la tabla ARP. A medida que las tramas se transmiten en la red, el dispositivo completa la tabla ARP con los pares de direcciones.

Otra manera en la que un dispositivo puede obtener un par de direcciones es emitir una solicitud de ARP. El ARP envía un broadcast de capa 2 a todos los dispositivos de la LAN Ethernet. La trama contiene un paquete de solicitud de ARP con la dirección IP del host de destino. El nodo que recibe la trama y que identifica la dirección IP como si fuera la suya responde enviando un paquete de respuesta de ARP al emisor como una trama unicast. Esta respuesta se utiliza entonces para crear una entrada nueva en la tabla ARP.

Estas entradas dinámicas de la tabla MAC tienen una marca horaria similar a la de las entradas de la tabla MAC en los switches. Si un dispositivo no recibe una trama de un determinado dispositivo antes de que venza la marca horaria, la entrada para este dispositivo se elimina de la tabla ARP.

Además, pueden ingresarse entradas estáticas de mapas en una tabla ARP, pero esto no sucede con frecuencia. Las entradas estáticas de la tabla ARP caducan cuando pasa el tiempo y deben eliminarse en forma manual.

Medios de transmisión guiados

En la unidad I se analizaron las definiciones de los medios que intervienen en las comunicaciones, se dividen en dos, guiados y no guiados, el primero que se enfocan a los medios que emplean cables y el segundo a los que usan el espectro para la transmisión de datos.

Par trenzado.

El medio de transmisión más antiguo es el par trenzado, que aún es muy usado hoy en día. Consiste en dos hilos de cobre aislados, de 1 mm de diámetro aproximadamente. los conductores se trenzan en forma helicoidal para reducir la interferencia eléctrica con respecto a los pares cercanos que se encuentran a su alrededor.

Debido a su buen comportamiento y bajo coste, están ampliamente difundidos. Por lo general se trata de 4 pares de cable conjuntos apantallados o no. Los tipos más utilizados y sus características son los siguientes:

- Sin apantallar (Unshielded Twisted Pair, **UTP**). 100 fi de impedancia característica.

  Tipo 3: 16 MHz de ancho de banda. Calidad telefónica. 7 a 10 cm por trenza.

  Tipo 4: 20 MHz de ancho de banda.

  Tipo 5: 100 MHz de ancho de banda. Calidad de datos. 0,5 a 1 cm por trenza.

- Apantallado (Shielded Twisted Pair, **STP**). 150 fi de impedancia característica. 300 MHz de ancho de banda.

  Las capacidades típicas que se suelen alcanzar son: 100 Mbps sobre 100 metros, 2 Mbps sobre 1500 metros y 60 kbps sobre líneas telefónicas. Las tasas de error están en torno a 1 bit entre cada millón.

Los cables de par trenzado utilizados para la instalación de redes locales se suelen denominar de categoría FTP y consisten en cuatro pares trenzados conjuntos que pueden tener o no apantallamiento según las necesidades de aislamiento. Permiten transmisiones a 100 Mbps a una distancia máxima recomendada de 100 m. para las cuales sólo se utilizan generalmente dos de los cuatro pares, uno para transmitir y otro para recibir.

Existen varios tipos de cables, se clasifican en Cable UTP, Cable FTP, Cable STP, Cable SSTP, Cable SFTP.

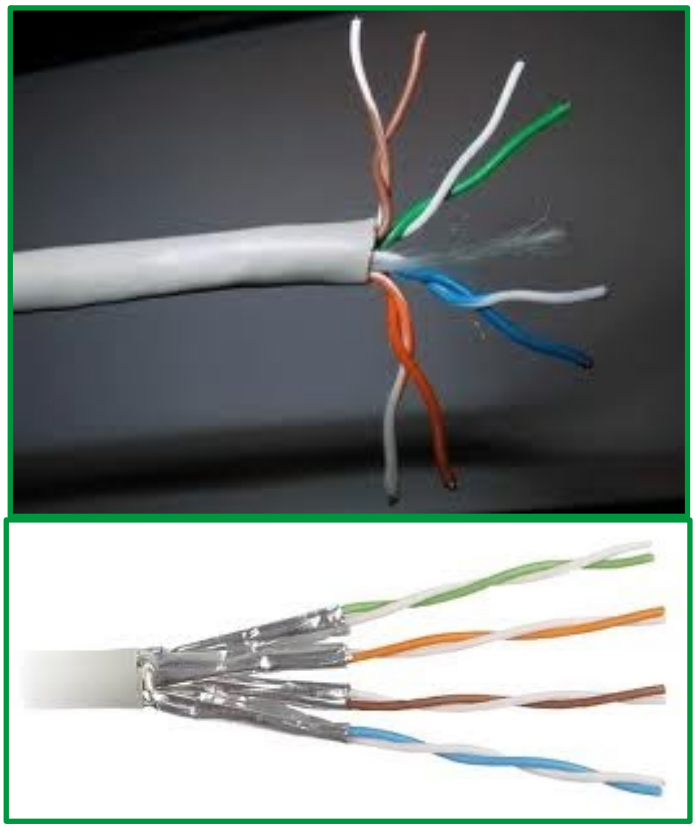


Figure 42:Cable par trenzado

Cable Coaxial.

El cable coaxial es otro medio típico de transmisión. Hay dos tipos de cable coaxial, el cable coaxial de 50 fi, que se usa en la transmisión digital y el cable coaxial de 75 fi que se emplea para la transmisión analógica. El cable de 50 fi también se conoce como cable coaxial de banda base, mientras que el 75 fi se denomina cable coaxial de banda ancha.

El cable coaxial consta de un alambre de cobre en su parte central o núcleo. Este se encuentra rodeado por un material aislante. A su vez, el material aislante está recubierto por un conductor que suele presentarse como una malla trenzada. Por último, dicha malla está recubierta por una capa de plástico protector. De este diseño en forma de capas concéntricas es de donde se deriva el nombre.

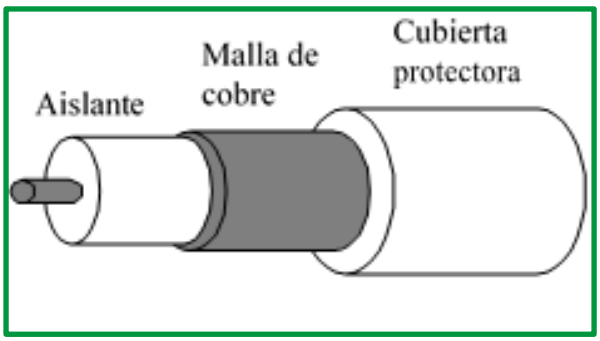


Figure 43:Cable Coaxial

El cable coaxial produce una buena combinación de un gran ancho de banda con una alta inmunidad al ruido. El ancho de banda que puede alcanzarse depende de la longitud del cable y del tipo, pudiendo ser de hasta 450 MHz. Así, un cable de 50 fi y de 1 km de longitud permite obtener velocidades de hasta 10 Mbps en banda base y hasta 150 Mbps en transmisiones en banda ancha sobre cables de 75 fi. Por otro lado, la señal eléctrica se propaga, según el tipo cable, a una velocidad que varía entre el 66% y el 80% de la velocidad de la luz. La atenuación de los cables varía entre los 20 y los 60 dB/100 m a 400 MHz.

- **Cable Coaxial Banda Base**.
  En las redes locales se suele usar el cable coaxial como bus de comunicación sobre el que se transmiten señales en banda base. El bus de cable coaxial ha de tener en cada extremo una resistencia con la impedancia característica del cable (p.ej. 50 fi) para evitar reflexiones en los mismos de la señal eléctrica que producirían interferencias e impedirían la comunicación. Ocasionalmente se utilizan en conexiones punto a punto sin necesidad del uso de terminadores.
  Existen dos formas de conectar ordenadores a un bus de cable coaxial: uso de conectores T o uso de conectores tipo vampiro. En el primer caso, hay que cortar el cable en dos partes e insertar una unión T, que vuelve a reconectar el cable y además proporciona una tercera conexión hacia el ordenador. El segundo tipo de conector consiste en hacer un orificio en el cable, de un diámetro y profundidad muy precisos, que atraviesa el cable hasta el núcleo. En el orificio se atornilla un conector especial que lleva a cabo la misma función de la unión en T, pero sin la necesidad de cortar el cable en dos.
  El hecho de incluir una unión en T implica realizar un corte en el cable y por tanto desconectar temporalmente la red. Para una red con un gran nivel de utilización, detenerla.
  cada vez que se conecta un nuevo equipo puede ser un gran inconveniente. Además, cuantos más conectores haya en el cable, más probabilidad existe de que alguna conexión sea defectuosa y ocasione problemas de vez en cuando.
  Los conectores tipo vampiro no ofrecen este problema, pero son más difíciles de instalar. Si el orificio es muy profundo puede llegar a romper el núcleo provocando falsos contactos. Por otra parte, si no es suficiente profundo, pueden provocarse falsos contactos debido al aislante. Además, los cables en este tipo de conexión son más gruesos y por tanto más caros.
- **Cable coaxial de banda ancha**.

  Este cableado se utiliza comúnmente para el envío de la señal de televisión por cable. El término banda ancha proviene del medio telefónico, y se refiere a frecuencias mayores a 4 kHz.

  Utilizan la tecnología patrón para envío de señales de televisión por cable y por ello pueden llegarse a alcanzar hasta 450 MHz de ancho de banda para longitudes de hasta 100 m. Un cable típico de 300 MHz puede, por lo general, mantener velocidades de hasta 150 Mbps. Es habitual que los sistemas de banda ancha se

dividan en varios canales, por ejemplo, en canales de 6 MHz para el envío de señal de televisión. Cada canal puede emplearse de forma independiente, por lo que en un mismo cable pueden coexistir señales de vídeo, voz y datos.

Una diferencia clave entre los sistemas de banda base y los de banda ancha es que los últimos necesitan amplificadores que repitan la señal en forma periódica. Estos amplificadores sólo pueden transmitir señales en una dirección de manera que un ordenador que de salida a un bloque de información sólo puede alcanzar a otros ordenadores que estén “aguas abajo”. Hay dos formas de solucionar este problema: uso de cable dual y uso de canales distintos.

En los sistemas de cable dual, se tienden dos cables idénticos paralelos. Para transmitir información el ordenador emplea uno de ellos, que envía el mensaje hacia el repetidor central (en la cabeza de la red). Una vez que el mensaje alcanza dicho repetidor se reenvía por el otro cable para que todos los ordenadores puedan leerlo.

El otro sistema consiste en aplicar diferentes frecuencias para las señales que entran y salen de un ordenador, sobre un cable sencillo. La banda de baja frecuencia se emplea para enviar información hacia el repetidor central para que éste la reenvíe hacia los ordenadores por la banda de mayor frecuencia. En el sistema de asignación baja el tráfico de llegada al repetidor usa una frecuencia de entre 5 y 30 MHz, mientras que el de salida usa una banda entre 40 y 300 MHz. En el sistema de asignación media, el tráfico entrante va entre 5 y 116 MHz, mientras que el de salida va entre 168 y 300 MHz. La adopción de estas técnicas se debe en parte a la fiabilidad y bajo coste del hardware empleado.

Un sistema de banda ancha puede usarse de diferentes maneras. Por ejemplo, se puede asignar un canal para su uso exclusivo por un par de ordenadores, mientras que los demás deben competir por el uso de un canal temporal mientras dure la comunicación. La forma en que se establece la competencia por el uso del canal se estudiará en la capa de enlace.

La instalación del sistema de banda base es simple, económica y emplea interfaces baratas. Ofrece un sólo canal digital con velocidades de unos 10 Mbps para distancias de 1 km. Son muy empleados para el diseño de redes locales.

La instalación del sistema de banda ancha requiere por lo general personal especializado, además, es necesario realizar un mantenimiento del sistema para asegurar que todos los repetidores están correctamente sintonizados. Por otra parte, un fallo en el repetidor central llevaría a la desconexión del sistema. Este resulta en general más costoso. Sin embargo, ofrece el uso de varios canales, aunque se limitan a unos 3 Mbps cada uno, y permite la transmisión simultánea de datos, voz y señales de televisión. En general, el ancho de banda adicional de estos sistemas no llega a justificar su complejidad y elevado coste, de manera que los sistemas de banda base son los de mayor uso.

Fibras ópticas.

Los avances en el campo de la tecnología óptica han hecho posible la transmisión de información mediante pulsos de luz. Un pulso de luz puede utilizarse para indicar un bit de valor 1, y su ausencia un bit de valor cero. La luz visible tiene una frecuencia de alrededor de 108 MHz, por lo que el ancho de banda de un sistema de este tipo tiene un potencial enorme.

Un sistema de transmisión óptica tiene 3 componentes: ***el medio de transmisión***, la ***fuente de luz*** y el ***detector***. El medio de transmisión es una fibra ultradelgada de vidrio o silicio fundido. También existen fibras fabricadas con polímeros plásticos de calidad inferior a las de vidrio. La fuente de luz puede ser un LED o un diodo láser; cualquiera de los dos emite luz cuando se le aplica una corriente eléctrica. El detector es un fotodiodo que genera un pulso eléctrico en el momento en el que recibe un rayo de luz. La transmisión de datos que se obtiene es unidireccional.

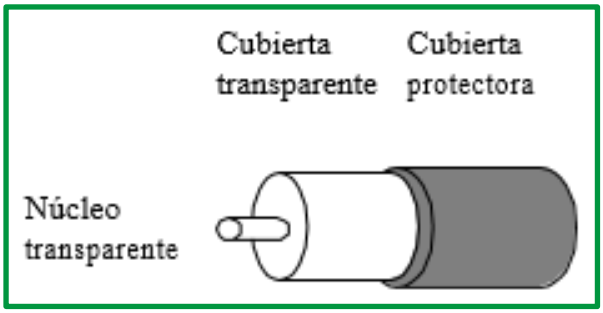


Figure 44:Fibra óptica

El sistema se basa en el principio físico de la refracción. Cuando un rayo de luz pasa de un medio a otro, el rayo se refracta en la frontera entre ambos medios. En general, el ángulo de refracción depende de las propiedades de los medios en contacto, en particular de sus índices de refracción. Si el ángulo de incidencia se encuentra por encima de un determinado valor crítico, la luz se refleja y no sale del medio.

La fibra óptica está compuesta por dos medios transparentes de distinto índice de refracción, un núcleo y un revestimiento que lo envuelve. Finalmente se cubre el conjunto con una cubierta opaca. Así, los rayos que incidan por encima del ángulo crítico van a quedar atrapados dentro del núcleo de la fibra, y pueden propagarse a lo largo de varios kilómetros sin apenas tener pérdidas.

Dado que cualquier rayo de luz incidente, por encima del ángulo crítico, se reflejará internamente, existirá una gran cantidad de rayos diferentes rebotando a distintos ángulos. A esta situación se la conoce como fibra multimodo. Si el índice de refracción es uniforme en todo el núcleo, la fibra se denomina de índice de escala y los haces rebotarán bruscamente en el punto de contacto del núcleo con el revestimiento, que tiene un índice de refracción diferente. Si el índice de refracción del núcleo varia gradualmente, aumentando poco a poco hacia el centro del mismo, la fibra se denomina de índice gradual y los haces de luz son

conducidos de forma más suave hacia el interior de la fibra, sin que reboten bruscamente reduciendo así las pérdidas en la propagación del haz.

Si el diámetro se reduce hasta que sea semejante al valor de la longitud de onda de la luz, la fibra actúa como una guía de ondas, y la luz se propaga en línea recta sin rebotar, produciendo así una fibra monomodo. Estas fibras necesitan diodos láser para su excitación, se asegura una mayor eficiencia y pueden usarse en distancias muy largas.

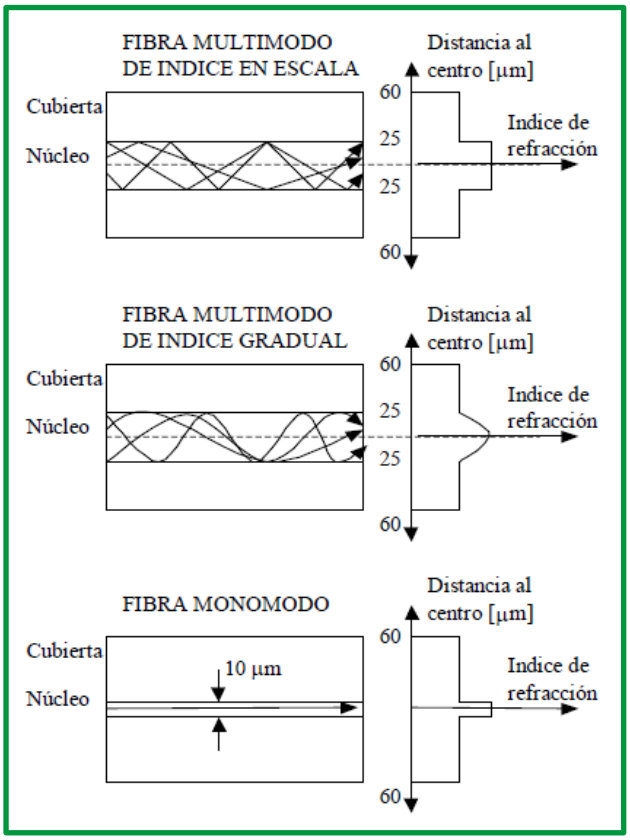


Figure 45: Fibra monomodo y multimodo

La ***apertura numérica*** de una fibra óptica es el parámetro que define el ángulo crítico para que la luz se propague a través de la fibra óptica. En concreto, la apertura numérica, NA, es seno del máximo ángulo respecto al eje longitudinal con el que un haz de luz puede incidir en el extremo de una fibra óptica para que se propague por la misma. Este parámetro está íntimamente relacionado con los diámetros del núcleo y el revestimiento. Cuanto más grandes sean estos, mayor es la apertura numérica y más fácil resultará el acoplamiento de dos segmentos de fibra óptica o de esta con los dispositivos emisor y receptor. Sin embargo, crecerán a la vez las pérdidas en la propagación de la luz.

Los enlaces de fibra óptica se están usando para la sustitución de enlaces telefónicos de larga distancia. Hasta ahora se usaba cable coaxial de banda ancha.

También se usan para el montaje de redes LAN, aunque requieren una tecnología más compleja que el cable coaxial. El problema fundamental es que la realización de conexiones intermedias es complicada y supone una importante pérdida de luz.

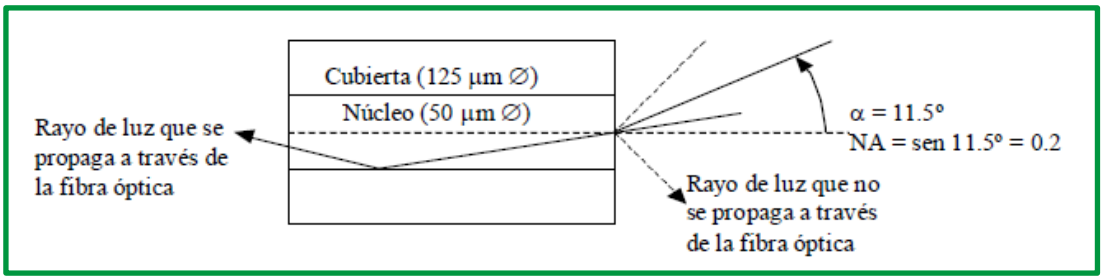


Figure 46:Apertura NA

Una red en forma de anillo es una solución al problema ya que es en realidad una colección de enlaces punto a punto. La interfaz que existe en cada ordenador permite el paso del flujo de los pulsos de luz al siguiente enlace y como unión en T por medio de la cual el ordenador envía y acepta mensajes.

Hay dos tipos de interfaz. Uno es de tipo pasivo. Está formado por dos conectores fusionados con la fibra principal, uno tiene un LED en su extremo (para transmisión) y el otro tiene un fotodiodo (para recepción). La conexión es completamente pasiva y por tanto muy fiable.

El otro tipo de interfaz es el receptor activo. La luz incidente se convierte en señal eléctrica y se regenera a su máximo valor, retransmitiéndose de nuevo como luz. Como en cada enlace se regenera la señal, cada línea puede tener varios kilómetros de longitud. En cambio, en un anillo pasivo, se pierde luz en cada enlace por lo que está limitado el número de estaciones y la longitud total del anillo. Entre las principales ventajas de la fibra óptica frente a otros tipos de cableado cabe destacar las siguientes:

- Mayor velocidad de propagación de la señal. La señal luminosa se propaga a la velocidad de la luz.
- Mayor capacidad de transmisión. En la actualidad se pueden hacer transmisiones de hasta 1 Gbps en distancias de 1 km.
- Inmunidad ante interferencias electromagnéticas.
- Menor atenuación. 5 a 20 dB/km a 400 Mhz.
- Mayor ancho de banda.
- Tasas de error menores. 1 error por cada 109 bits frente a 1 por cada 106 en los cables eléctricos.
- No hay riesgos de cortocircuitos o daños de origen eléctrico.
- Peso mucho menor.
- Menor diámetro y más flexibles lo que facilita su instalación.
- Es más difícil realizar escuchar sobre una fibra óptica que sobre un cable eléctrico.
- Se pueden emplear varios canales empleando longitudes de onda diferentes simultáneamente sobre la misma fibra.
- Tiene mayor resistencia a los ambientes corrosivos que los cables eléctricos.
- Las materias primas para su fabricación son abundantes.
- Su vida media es mucho más larga que la de un cable eléctrico.

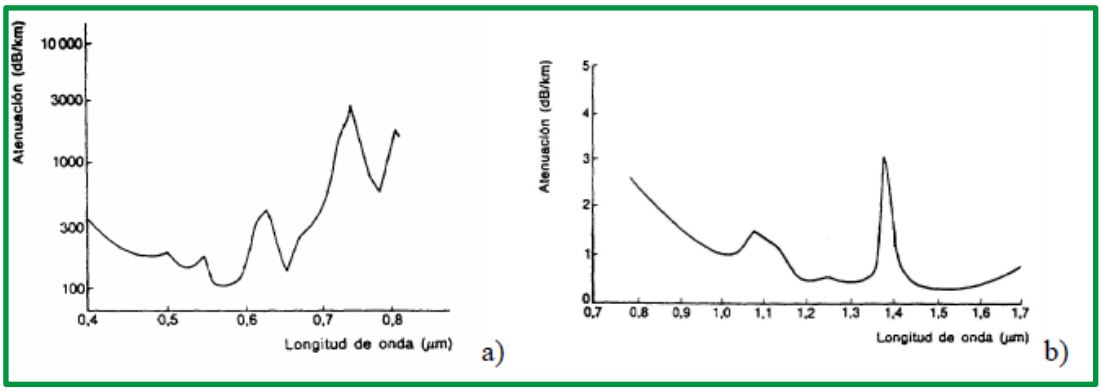


Figure 47: atenuación de fibra óptica: a) de polímeros – b) monomodo de cristal

Sin embargo, también presentan inconvenientes. Por un lado, las fibras ópticas son inherentemente unidireccionales y el coste de las interfaces es mucho mayor que en el caso eléctrico. Por otro lado, la unión de fibras ópticas es complicada y todavía más su derivación. Uno de los elementos más costosos de una instalación de fibra óptica es la incorporación de las férulas de conexión en los extremos de las fibras. Las férulas suelen ser complejas y de laboriosa instalación. De la delicada y correcta instalación de estas férulas, depende el correcto alineamiento entre los extremos de las dos fibras que se vayan a conectar o del extremo de la fibra con los dispositivos emisor o receptor. Si el alineamiento no es correcto, la limitada apertura numérica de una fibra puede impedir total o parcialmente la propagación de la señal luminosa.

Transmisión inalámbrica.

La transmisión inalámbrica transmite y reciben señales electromagnéticas sin un conductor eléctrico u óptico, las ondas electromagnéticas son el medio de trasmisión, existen diferentes medios de transmisión como radio enlace, luz infrarroja, microondas.

Transmisión por trayectoria óptica

Los sistemas por trayectoria óptica son básicamente un enlace de fibra óptica en el que se ha sustituido esta por el aire. La transmisión de datos puede realizarse mediante rayos infrarrojos para distancias cortas y láser para distancias de hasta unos 2 km.

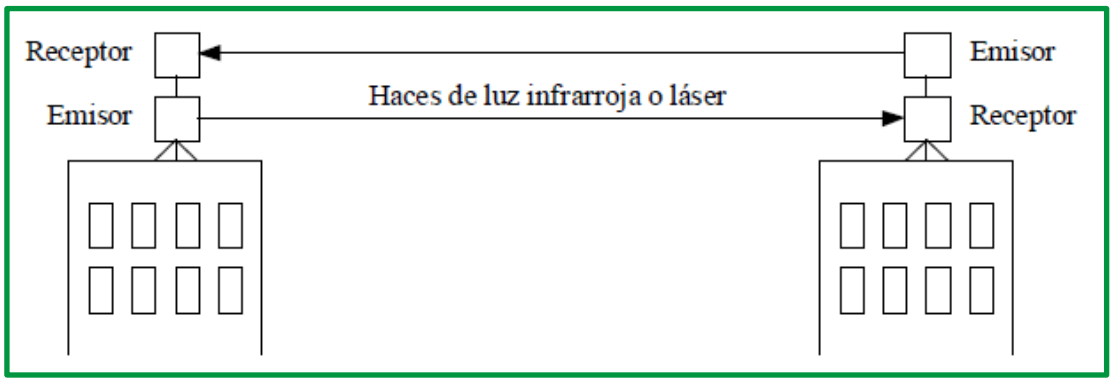


Figure 48:Trasmisión óptica

Como la transmisión es eminentemente unidireccional, es preciso que en cada extremo del enlace exista un transmisor y un receptor dotados de una óptica adecuada para un óptimo enfoque.

Por ejemplo, en el tendido de una red LAN a través de varios edificios de un campus o de una compañía, usar un cable para unirlos, puede resultar caro e incluso inconveniente. Una solución puede ser el empleo de enlaces ópticos al aire libre por láser desde las azoteas de los edificios. Son fáciles y rápidos de instalar, no requieren permisos de las autoridades de telecomunicaciones, son inmunes a interferencias eléctricas y se pueden transmitir voz y datos hasta 45 Mbps.

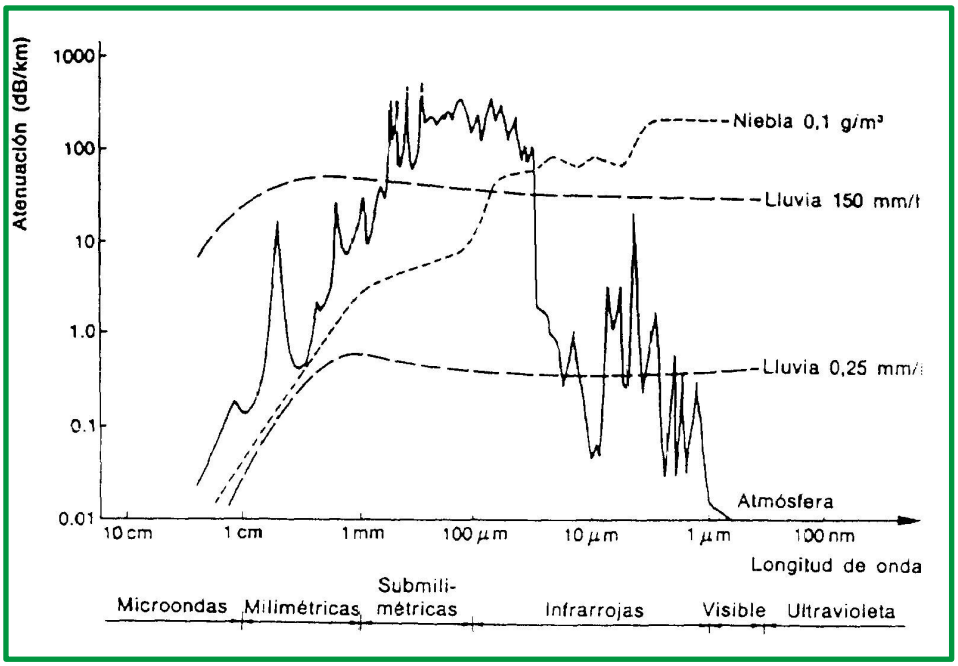


Figure 49:: Fenómenos que afectan las comunicaciones ópticas

La comunicación por láser o infrarrojo es totalmente digital, altamente directiva y en consecuencia las partículas en suspensión en la atmósfera como la lluvia o la niebla pueden ocasionar interferencia en la comunicación en función de la longitud de onda elegida. Además, las brisas ascensionales provocadas por variaciones de temperatura que modifican la densidad del aire, provocan desviaciones del haz de luz evitando que incida correctamente en el receptor. La utilización de la luz coherente del láser añade el peligro de los posibles daños en la retina si es enfocada en el ojo humano.

Enlaces por radio y microondas

Todas las frecuencias del espectro radioeléctrico pueden ser utilizadas para la transmisión de datos, aunque las microondas resultan especialmente adecuadas.

En aplicaciones de comunicaciones a larga distancia se ha empleado la transmisión por radio de microondas. Las antenas parabólicas se pueden montar sobre torres para enviar un haz de señales a otra antena a decenas de kilómetros de distancia. El sistema es muy usado en

transmisiones telefónicas y de vídeo. Cuanto más alta sea la torre mayor es el alcance ya que se propagan fundamentalmente en línea recta.

La transmisión mediante microondas se lleva a cabo en una escala de frecuencias que va de 2 a 40 GHz. Estas frecuencias se han dividido en bandas de portadoras para uso gubernamental, militar, etc. Con una torre de 100 m pueden llegar a cubrirse distancias de 100 km. La atenuación es tanto mayor cuanto mayor es la frecuencia.

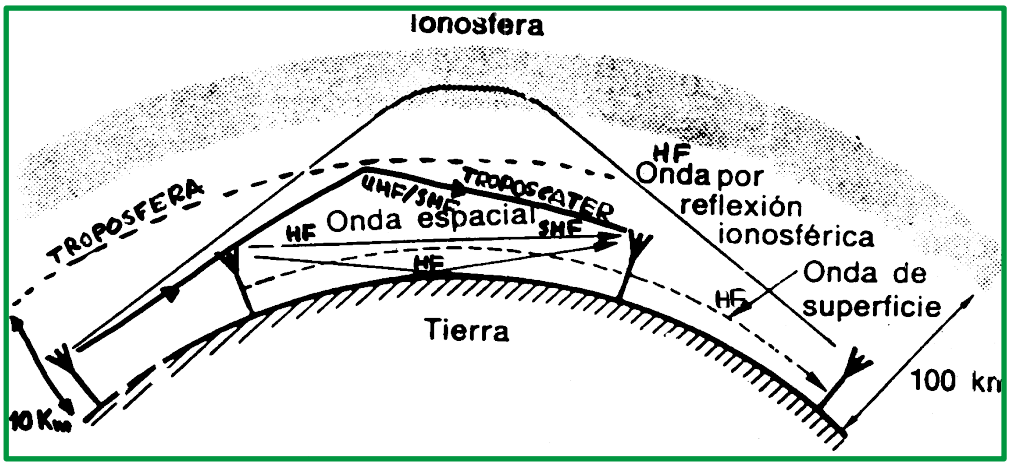


Figure 50: Tipos de Ondas

Otras ondas pueden propagarse de distintas maneras permitiendo alcanzar mayores distancias como en el caso de las ondas de alta frecuencia (HF). Según la forma en que se propagan se tienen los siguientes tipos de ondas:

- **Ondas espaciales**: Es la forma en que se propagan la mayoría de las ondas, en línea recta o con una simple reflexión sobre la superficie terrestre (que a veces puede ser perjudicial y provoca ecos de la señal).
- **Ondas de superficie**: Algunas frecuencias de la banda de HF tienen la propiedad de propagarse siguiendo la curvatura de la superficie terrestre, lo que les permite alcanzar mayores distancias.
- **Ondas ionosféricas**: Se trata de ondas capaces de reflejarse en la ionosfera, una capa de la atmósfera terrestre situada a 100 km de altura. Algunas frecuencias de la banda HF alcanzan grandes distancias gracias a esta propiedad.
- **Troposcater**: Frecuencias de las bandas UHF y SHF (microondas) tienen la propiedad de ser reflejadas por una capa de la atmósfera terrestre denominada troposfera a 10 km sobre la superficie terrestre.

La actual proliferación de dispositivos inalámbricos ha dado lugar a un nuevo desarrollo de las transmisiones vía radio. Desde los sistemas de telefonía móvil GSM/GPRS en las bandas de 800 y 1800 MHz (1900 MHz en EEUU) hasta los equipos informáticos que usan fundamentalmente la banda de microondas de 2,4 GHz para transmisiones Bluetooth, WLAN (Wireles LAN) o Wi-Fi (Wíreles Fidelity), y HomeRF.

En cada uno de estos sistemas los métodos de multiplexación y modulación se complican. En GSM el esquema de multiplexación de canales se basa en FH (salto de frecuencia, Frequency Hopping) mezclado con FDMA (multiplexación en frecuencia, Frequency Division Multiple Access) y TDMA (multiplexación en el tiempo, Time Division Multiple Access) con modulación GMSK (Gaussian Minimun Shift Keying).

En las WLAN se usan técnicas de modulación de espectro disperso: FHSS (Frequency-Hopping Spread Spectrum) y DSSS (Direct-Sequence Spread Spectrum). La multiplexación para el acceso al medio en las WLAN se realiza mediante CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

Frecuencia Hz (aprox.)	Longitud de onda	Denominación	Aplicaciones
>3.000 G	<100 μm	Infrarrojo	Enlaces de datos.
300 G – 3.000 G	1 mm – 100 μm	THF Frecuencias Tremendamente Altas (ondas submilimétricas)	
30 G – 300 G	1 cm – 1 mm	EHF Frecuencias Extremadamente Altas (ondas milimétricas)	Radar, enlaces de datos.
3 G – 30 G	10 cm – 1 cm	SHF Frecuencias Super Altas (microondas)	Radar, comunicaciones por microondas.
300 M – 3 G	1 m – 10 cm	UHF Frecuencias Ultra Altas	Televisión, comunicaciones móviles de corto alcance.
30 M – 300 M	10 m – 1 m	VHF Frecuencias Muy Altas	Radiodifusión FM, comunicaciones móviles de corto alcance.
3 M – 30 M	100 m – 10 m	HF Frecuencias Altas	Radiodifusión, comunicaciones de larga distancia.
300 k – 3 M	1000 m – 100 m	MF Frecuencias Medias	Radiodifusión, comunicaciones de medio alcance.
30 k – 300 k	10 km – 1000 m	LF Frecuencias Bajas	Radiodifusión.
3 k – 30 k	100 km – 10 km	VLF Frecuencias Muy Bajas	Telegrafía de larga distancia y navegación.
300 – 3 k	1000 km – 100 km	ILF Frecuencias Super Bajas	
<300	>1000 km	ELF Frecuencias Ultra Bajas	

Figure 51: Tabla de análisis de frecuencia y aplicaciones

Comunicación por satélite

Los primeros satélites de comunicaciones se emplearon de forma experimental por la NASA en 1960. Se trataba de unos simples globos de mylar aluminado, de unos 33 metros de diámetro, denominados Echo I y Echo II ya que actuaban como simples reflectores pasivos. En ese mismo año se lanzaron los primeros satélites activos.

En la actualidad este tipo de comunicación puede imaginarse como si tuviésemos un enorme repetidor de microondas en el cielo. Está constituido por uno o más dispositivos receptor-transmisor, cada uno de los cuales escucha una parte del espectro, amplificando la señal de entrada y retransmitiendo a otra frecuencia para evitar los efectos de interferencia. El flujo hacia la tierra puede ser muy amplio y cubrir una parte significativa de la superficie terrestre, o bien ser pequeño y cubrir un área de unos cientos de kilómetros de diámetro.

Habitualmente, la mejor órbita de los satélites de comunicaciones es una órbita geoestacionaria. Con la tecnología actual no es deseable tener satélites espaciados a menos de 4º. El haz proveniente de la tierra, considerando separaciones menores, iluminaría al que

se desea y también a los que le rodean. Con este espaciamiento sólo puede haber 90 satélites geoestacionarios al mismo tiempo y el problema es aún más grave en el cuadrante más utilizado, el que se encuentra sobre EEUU y Europa.

Debido a su gran potencia, los satélites de TV necesitan un espaciado de 8º. Hay una gran competencia por el uso de los mismos. Dos satélites que operen en bandas de frecuencia distintas, si pueden ocupar la misma ranura espacial.

Existen acuerdos internacionales para el uso de ranuras orbitales y frecuencias. Las bandas de 3.7 a 4.2 GHz y de 5.925 a 6.425 GHz se han asignado como frecuencias de telecomunicación vía satélite para flujos provenientes del satélite o dirigidos hacia él. En la actualidad estas bandas están superpobladas porque también se utilizan por los proveedores de servicios portadores para enlaces terrestres de microondas.

Las bandas superiores siguientes que se encuentran disponibles son las de 12-14 GHz, y a estas frecuencias los satélites pueden tener un espaciado de 1º. El problema en este caso es la lluvia, ya que el agua es un gran absorbente de este tipo de microondas. Las bandas de 20-30 GHz también se han reservado para comunicaciones por satélites, pero el coste de la tecnología necesaria resulta prohibitivo.

Un satélite típico divide su ancho de banda de 500 MHz en unos 12 receptores- transmisores de un ancho de banda de 36 MHz cada uno. Cada par puede emplearse para codificar un flujo de información de 50 Mbps, 800 canales de voz digitalizada de 64 kbps, o bien, otras combinaciones diferentes.

En los primeros satélites, la división en canales era estática separando el ancho de banda en bandas de frecuencias fijas. En la actualidad el canal se separa en el tiempo, primero una estación, luego otra, y así sucesivamente. El sistema se denomina de multiplexión por división en el tiempo. También tenían un solo haz espacial que cubría todas las estaciones terrestres. Con los desarrollos experimentados en microelectrónica, un satélite moderno posee múltiples antenas y pares receptor-transmisor. Cada haz de información proveniente del satélite puede enfocarse sobre un área muy pequeña de forma que pueden hacerse simultáneamente varias transmisiones hacia o desde el satélite. A estas transmisiones se les llama traza de ondas dirigidas. La información transmitida a través del satélite sufre un retardo adicional como consecuencia de la larga distancia que debe recorrer la señal. Este tiempo extremo a extremo oscila entre 250 y 300 ms.

Los enlaces terrestres tienen un retardo de propagación de unos 3 µs/km. en un cable coaxial el retardo es de unos 5 µs/km (la velocidad de la señal eléctrica en el cobre es menor que la de la electromagnética en el aire). El retardo total depende del ancho de banda y la tasa de errores. Así, para x kbits enviados por un enlace terrestre de 9600 bps se emplean x/9.6 segundos. Para enviar la misma información por satélite, a una velocidad de 5 Mbps se emplean (x/5000+0.270) segundos, incluyendo el retardo de propagación. Para x>2.6 kbits, la transmisión vía satélite es más rápida. Si además incluyera la tasa de errores, el resultado es aún más favorable para el satélite. Además, la tarifa es independiente de la distancia.

Otra propiedad interesante del envío de datos por satélite es su difusión. Todas las estaciones incluidas bajo el área del haz, pueden recibir la comunicación, incluso las estaciones piratas. Las implicaciones en cuanto a la privacidad son inmediatas. Es necesario alguna forma de encriptación para mantener el secreto de las comunicaciones privadas.

En cuanto a los fenómenos que dificultan las comunicaciones vía satélite, se han de incluir también el movimiento aparente en 8 de los satélites de la órbita geoestacionaria debido a los balanceos de la Tierra en su rotación, los eclipses de sol en los que la tierra impide que el satélite pueda cargar baterías con sus células solares y los tránsitos solares, en los que el sol interfiere las comunicaciones del satélite al encontrarse este en la trayectoria entre el sol y la tierra.

Modulación digital y multiplexación.

Modulación Digital

Es la modulación de una portadora senoidal por una señal digital. Es decir, lo que distingue esta modulación de la analógica, es que la modulante es una señal digital. Se pueden distinguir dos tipos de situaciones en que se la utiliza:

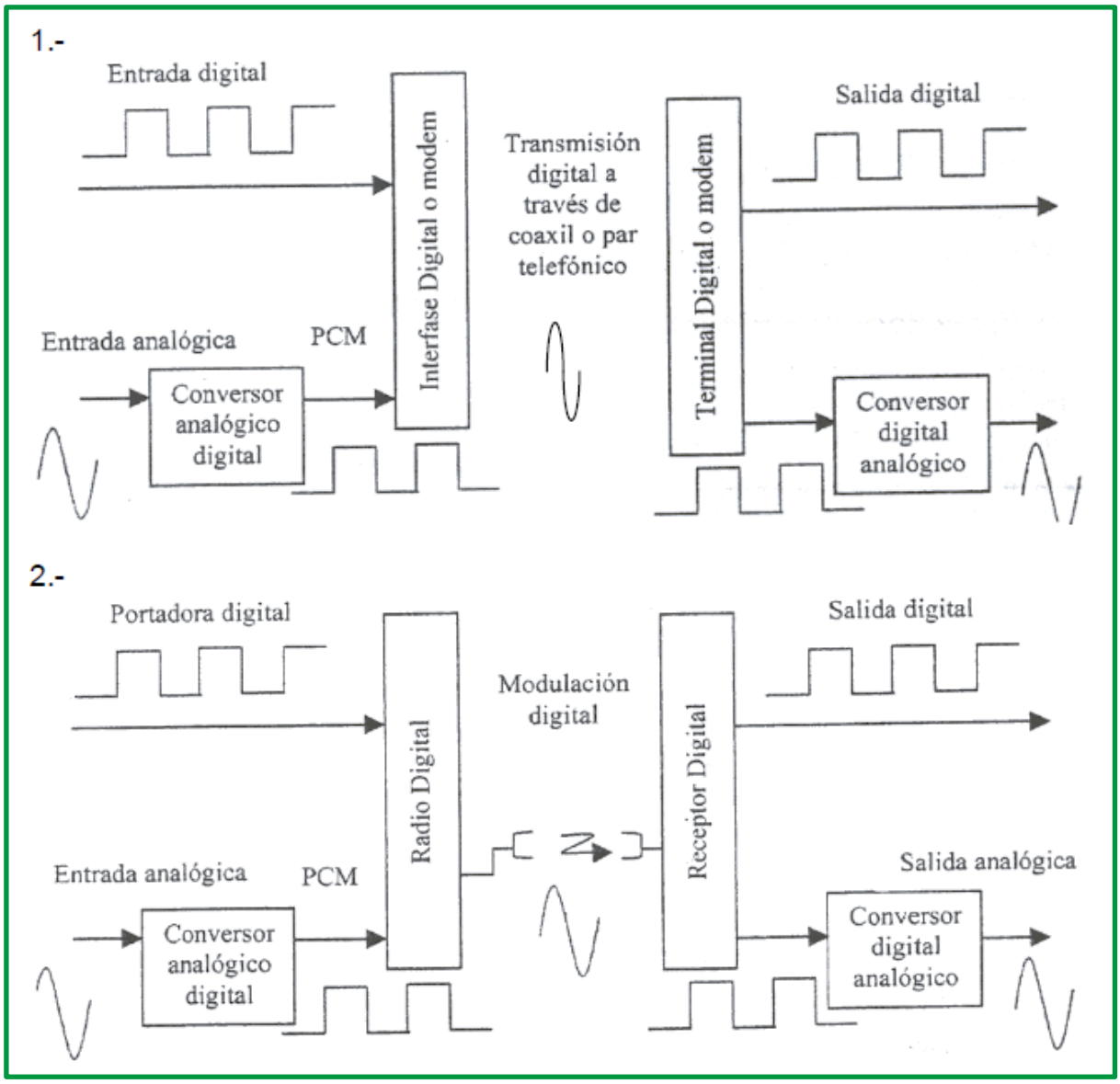


Figure 52: Aplicación de modulación digital

De igual forma que la modulación analógica, se aplican las tres formas básicas de varias la portadora (amplitud, frecuencia y fase), se denominan como:

- Modulación por desplazamiento de amplitud (ASK, Amplitude Shift Keying)
- Modulación por desplazamiento de frecuencia (FSK,Frecuency Shift Keying)
- Modulación por desplazamiento de fase (PSK, Phase Shift Keying)
- **QAM** (quadrature amplitude modulation) o modulación de amplitud en cuadratura, es una combinación de ASK y PSK

Todas estas formas tienen variantes, dependiendo si se utiliza señalización binaria o señalización multinivel. En sí misma la QAM es una señalización multinivel o una modulación multisimbólica.

En la señalización binaria, la señal portadora toma el valor 1 o el valor O, dependiendo de la modificación efectuada. Como se ve, los bits se toman de a uno.

En la señalización multinivel o multisimbólica, en vez de tomar los bits de a uno, se los agrupa de a 2, de a 3, de a 4, etc. Entonces cada vez que se modifica la señal portadora se está enviando mayor cantidad de información (2. 3. o 4 bits, etc).

Modulación por desplazamiento de amplitud (ASK, Amplitude Shift Keying)

Forma de modulación digital que consiste en cambiar la amplitud de una onda portadora (una sinusoide) entre dos valores posibles.

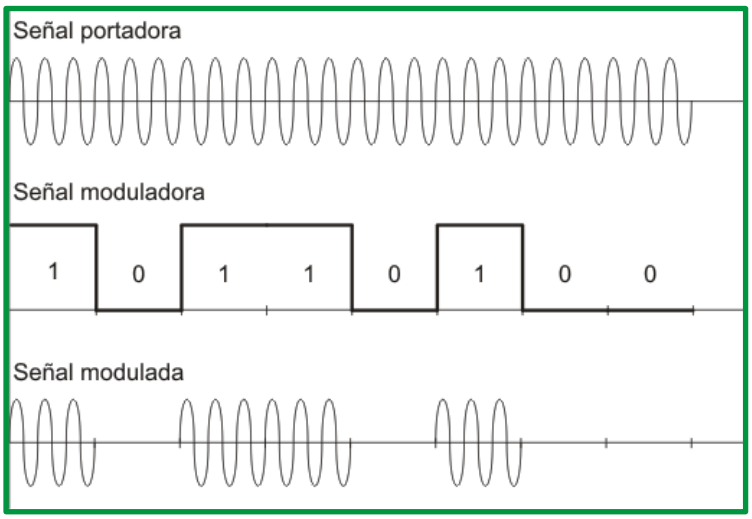


Figure 53: Técnica ASk

Es una modulación de amplitud donde la señal moduladora (datos) es digital. Los dos valores binarios (0 y 1) se representan con dos amplitudes diferentes y es usual que una de las dos amplitudes sea cero; es decir uno de los dígitos binarios se representa mediante la presencia de la portadora a amplitud constante, y el otro dígito se representa mediante la ausencia de la señal portadora, en este caso la frecuencia y la fase se mantiene constante.

La modulación en ASK no es otra cosa que una variante de la modulación en AM que se adapta perfectamente a las condiciones de los sistemas digitales, además de que les permite trabajar sobre una sola frecuencia de transmisión en vez de tener que lidiar con pulsos cuadrados que contienen componentes en todas las frecuencias del espectro.

Su recuperación también resulta ser más sencilla, dado que sólo depende de sincronizar la frecuencia de las señales sinusoidales que sirven de portadoras y regeneradoras dependiendo si se hallan en el modulador o el demodulador.

El ASK por sí sólo, a pesar de todas estas consideraciones, no es uno de los métodos más utilizados debido a que para cada frecuencia es necesario realizar un circuito independiente, además de que sólo puede transmitirse un solo bit al mismo tiempo en una determinada frecuencia. Otro de los inconvenientes es que los múltiplos de una frecuencia fundamental son inutilizables y que este tipo de sistemas son susceptibles al ruido.

La técnica ASK se utiliza para la transmisión de datos digitales en fibras ópticas, en los transmisores con LED.

Modulación por desplazamiento de frecuencia (FSK,Frecuency Shift Keying)

Es una técnica de transmisión digital de información binaria (ceros y unos) utilizando dos frecuencias diferentes. La señal moduladora solo varía entre dos valores de tensión discretos formando un tren de pulsos donde un cero representa un "1" o "marca" y el otro representa el "0" o "espacio".

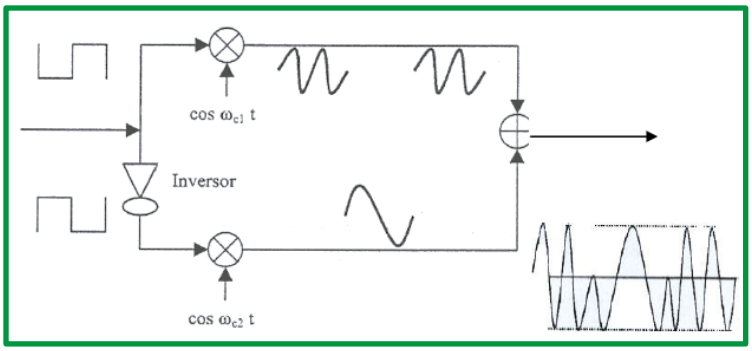


Figure 54:Generación FSK

En la modulación digital, a la relación de cambio a la entrada del modulador se le llama bit-rate y tiene como unidad el bit por segundo (bps).

A la relación de cambio a la salida del modulador se le llama baud-rate. En esencia el baud-rate es la velocidad o cantidad de símbolos por segundo.

En FSK, el bit rate = baud rate. Así, por ejemplo, un 0 binario se puede representar con una frecuencia f1, y el 1 binario se representa con una frecuencia distinta f2.

Modulación por desplazamiento de fase (PSK, Phase Shift Keying)

La modulación PSK se caracteriza porque la fase de la señal portadora representa cada símbolo de información de la señal moduladora, con un valor angular que el modulador elige entre un conjunto discreto de "n" valores posibles.

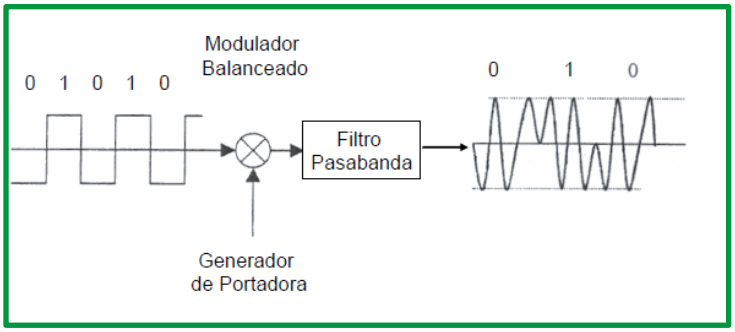


Figure 55:Generación PSK

La modulación PSK también se denomina “por desplazamiento” debido a los saltos bruscos que la moduladora digital provoca en los correspondientes parámetros de la portadora.

Un modulador PSK representa directamente la información mediante el valor absoluto de la fase de la señal modulada, valor que el demodulador obtiene al comparar la fase de esta con la fase de la portadora sin modular.

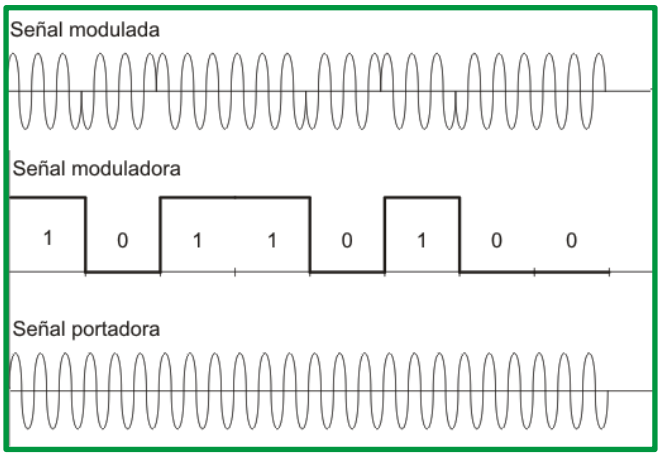
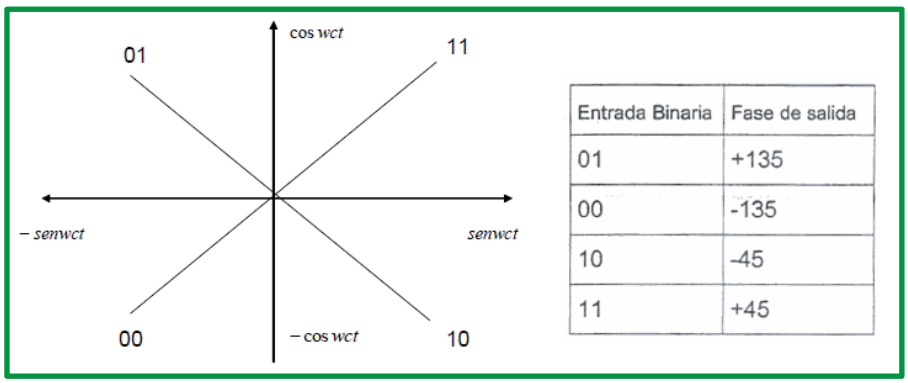


Figure 56: Técnica de modulación PSK

La multiplexación en la técnica que combina dos o más canales para trasmitir información en un solo medio, es decir, un canal de comunicación lleva varias transmisiones al mismo tiempo usando un dispositivo llamado multiplexor. El proceso inverso se conoce como demultiplexación.

- **QPSK o modulación por desplazamiento de fase cuaternaria.**

En este sistema, en la entrada los bits se transmiten de a dos, en "dibits", lo que se pretende es producir un cambio en la salida cada dos bits. Como se pueden formar cuatro combinaciones distintas con dos bits, se tienen cuatro fases distintas para la misma frecuencia portadora, que mantiene, además, al menos idealmente, su amplitud constante.



Entrada Binaria	Fase de salida
01	+135
00	-135
10	-45
11	+45

Figure 57: Fases cuaternaria

Si se expresa analíticamente las fases tenemos:

11: + sen wct + cos wct
01: - sen wct – cos wct
00: - sen wct – cos wct
10: + sen wct – cos wct

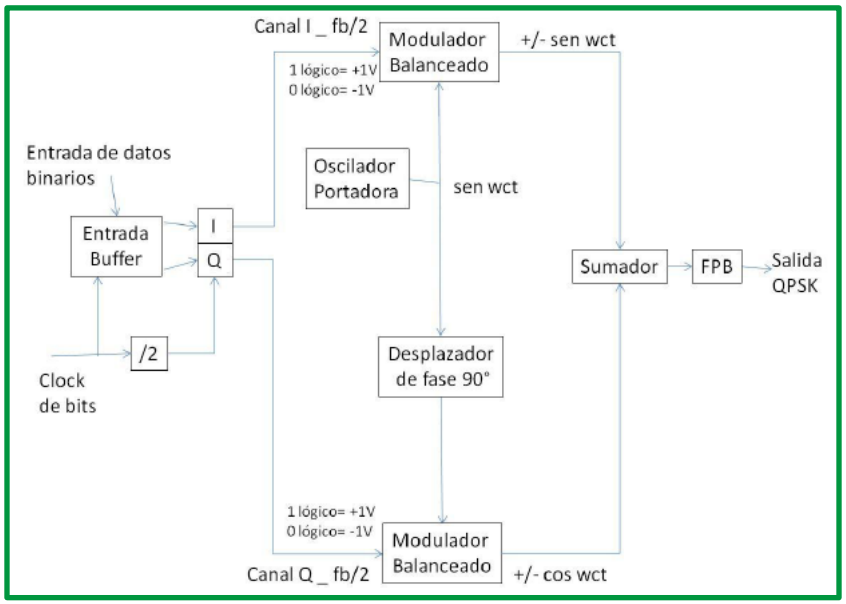


Figure 58:Generación QPSK

- **8PSK.** En este caso, se toman los bits de a tres, formando un "tribits". Las fases están diferenciadas en 45°. Se muestra el diagrama de constelación, siempre se forma un círculo.
- **16PSK.** Los bits se toman de a cuatro "cuadribits". La separación entre fases es de 22,5°. La tasa de baudios y el ancho de banda son de 1/4 de la tasa de bits.
- **DBPSK –Modulación por Desplazamiento de Fase Binaria Diferencial.** Esta técnica se utiliza para evitar proveer portadora sincrónica en el receptor y demodular la señal mediante un circuito cuadrador o recuperador de la portadora.

QAM o modulación de amplitud en cuadratura

Es una forma de modulación digital donde la información está contenida en la amplitud y en la fase de la señal transmitida.

Al igual que QPSK, 8PSK, 16PSK es una operación del tipo multinivel, en la cual, al combinar modulación en fase y amplitud se intenta mejorar el comportamiento frente al ruido.

Existen varias versiones actuales de hasta 1024QAM, solo se mostrarán a título de ejemplo 8QAM y 16QAM.

- 8QAM. Los datos se agrupan de a tres, resultando el siguiente diagrama de constelación, en el cual se visualizan dos amplitudes y cuatro fases diferentes. La tasa de señalización es 1/3 de la de bits.

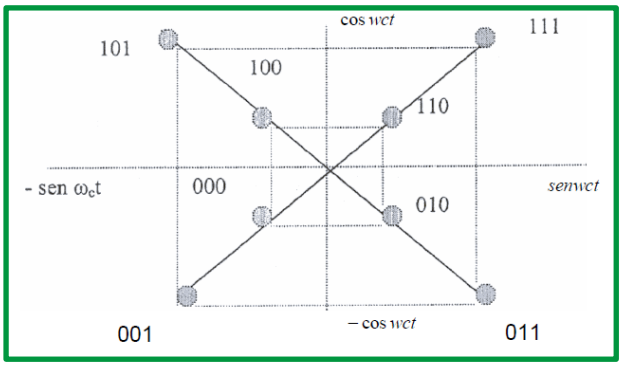


Figure 59. Diagrama de constelación 8QAM

- 16QAM. En el 16 QAM hay 3 amplitudes distintas y 12 fases diferentes

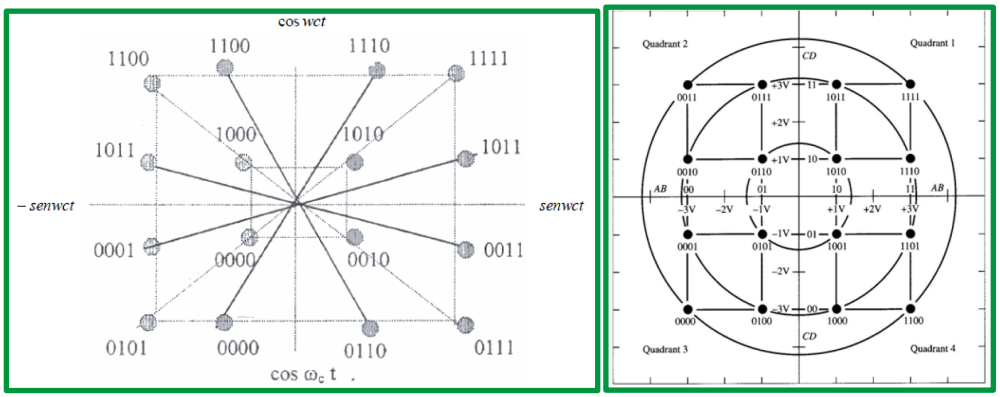


Figure 60:Diagrama de constelación 16QAM

MODULACIÓN	CODIFICACION	BW en Hz	EFICIENCIA de BW Bits/Hz
FSK	BIT UNICO	>Fs	1
BPSK	BIT UNICO	Fs	1
QPSK	DIBIT	Fb/2	2
8 PSK	TRIBIT	Fb/3	3
8 QAM	TRIBIT	Fb/3	3
16 PSK	QUADBIT	Fb/4	4
16 QAM	QUADBIT	Fb/4	4

Figure 61: Tabla de comparación de BW y eficiencia de la modulación digital

Multiplexación

El término multiplexación hace referencia al proceso mediante el cual diferentes mensajes de información (como conversaciones telefónicas, transmisión simultánea de audio + vídeo + datos o diferentes canales de audio) generados típicamente en una misma ubicación física, se combinan en una única señal con el fin de compartir un recurso de comunicaciones. Es la combinación de dos o más canales de información en un solo medio de transmisión que aplica un dispositivo llamado multiplexor.

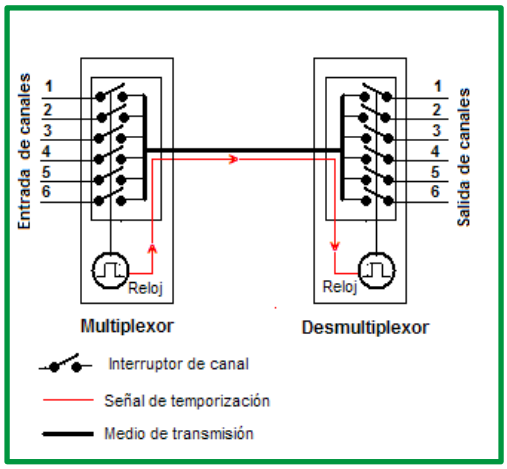


Figure 62:Multiplexor y desmultiplexor

La multiplexación tiene como objetivos compartir la capacidad de transmisión de datos sobre el mismo enlace para aumentar la eficiencia y el de minimizar las cantidades de líneas físicas necesarias maximizando el uso del ancho de banda del medio. Entre los tipos de multiplexación tenemos:

- La multiplexación por división de tiempo o TDM
- La multiplexación por división de frecuencia o FDM
- La multiplexación por división en código o CDM
- La multiplexación por división de onda o WDM

Multiplexión por división de frecuencia (FDM)

La Multiplexión por División de Frecuencia (FDM) consiste en dividir mediante filtros el espectro de frecuencias del canal de transmisión y desplazar la señal a transmitir dentro del margen del espectro correspondiente mediante modulaciones, con lo cual cada usuario tiene posesión exclusiva de su banda de frecuencia. En este tipo de multiplexión el espectro de frecuencias está representado por el ancho de banda disponible de un canal, se divide en porciones de ancho de banda más pequeños de acuerdo a la cantidad de canales de entrada los cuales se llaman subcanales.

Los subcanales se separan entre sí por una banda de guarda para evitar las interferencias por solapamiento. El tipo de multiplexión FDM modula cada señal para su transmisión; las señales pueden ser analógicas o digitales, para las analógicas se utilizan los tipos de modulación: AM, FM y PM; en el caso de las digitales utilizan ASK, FSK, PSK y DPSK.

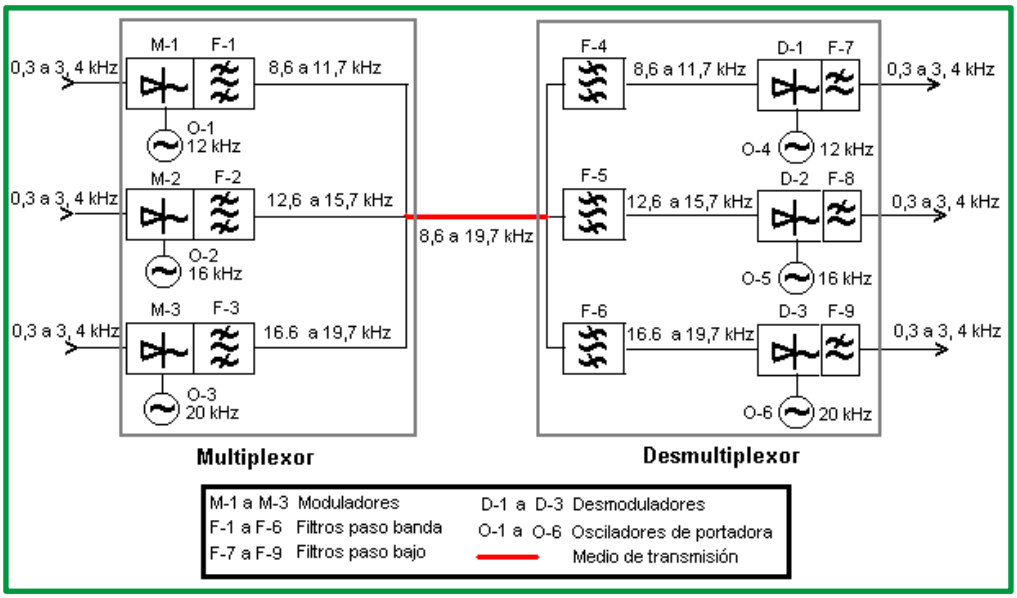


Figure 63: Diferentes canales, se modula diferentes portadoras.

Ventajas

- El usuario puede ser añadido al sistema añadiendo otro par de modulador y demodulador.
- El sistema de FDM apoya el flujo de dúplex total de información que es requerido por la mayor parte de la aplicación.
- El problema del ruido para la comunicación análoga tiene menos efecto en este tipo de sistema.

Desventajas

- El costo inicial es alto. Este puede incluir el cable entre los dos finales y los conectores asociados para el cable.
- El problema de un usuario puede afectar a veces a otros.
- Cada usuario requiere una frecuencia portadora precisa.

Multiplexión por división de tiempo (TDM)

La multiplexión por división de tiempo (TDM) es un medio de transmitir varios canales de información en el mismo circuito de comunicación utilizando la técnica de tiempo compartido, esta técnica es más utilizada en la actualidad, especialmente en los sistemas de transmisión digitales. El ancho de banda total del medio de transmisión es asignado a cada canal durante una fracción del tiempo total (intervalo de tiempo).

El multiplexor por división en el tiempo muestrea, o explora, cíclicamente las señales de entrada (datos de entrada) de los diferentes usuarios, y transmite las tramas a través de una única línea de comunicación de alta velocidad. Funcionan a nivel de bit o a nivel de carácter, a nivel de bit cada trama contiene un bit de cada dispositivo explorado; a nivel de caracteres manda un carácter en cada canal de la trama. El segundo es generalmente más eficiente, dado que requiere menos bits de control que un TDM de bit. La operación de muestreo debe

ser lo suficientemente rápida, de forma que cada buffer sea vaciado antes de que lleguen nuevos datos.

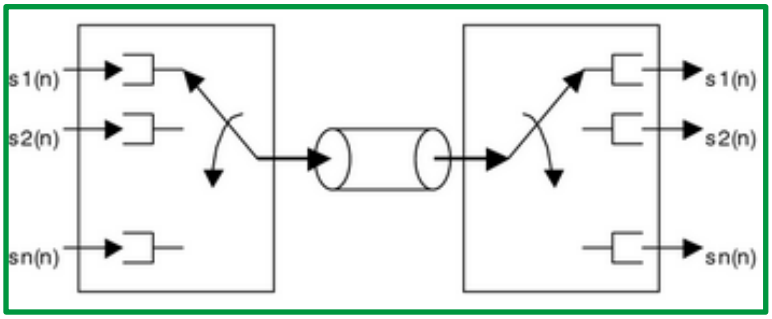


Figure 64:Esquema de multiplexación TDM

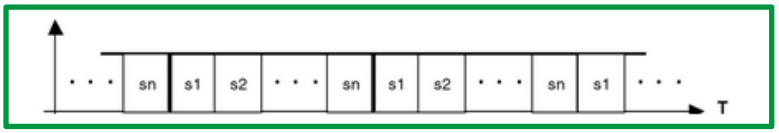


Figure 65: Separación en el tiempo de las señales multiplexadas mediante TDM

El Acceso múltiple por división de tiempo (TDMA) es una de las técnicas de TDM más difundidas.

Ventajas

- Bajo costo.
- Reducido tamaño de los equipos terminales.
- Inmunidad a las no linealidades de amplitud del enlace.
- Los canales telefónicos individuales pueden ser insertados y extraídos.

Desventajas

- Los sistemas TDM no se pueden interconectar a los FDM de similar capacidad.
- El costo inicial es alto.
- Mayor complejidad técnica.
- El problema del ruido para la comunicación análoga tiene mayor efecto.
- No permiten la transmisión de grandes grupos de canales telefónicos, pues se necesitarían pulsos muy estrechos y un amplio ancho de banda.

Multiplexación por división de código (CDM).

Es una técnica donde cada canal transmite sus bits como una secuencia de pulsos codificada de forma única para ese canal. Se consigue transmitiendo una serie de pulsos cortos. Esto permite transmitir por una misma fibra varios canales con códigos diferentes. Este tipo de multiplexación es compleja y es más conocida su variante de acceso múltiple (Code División Multiple Access, CDMA).

FDMA. Se denomina acceso múltiple por división de frecuencias (FDMA / Frequency Division Multiple Access). El ancho de banda disponible es dividido en una serie de canales que son asignados bien sea para transportar señales de control o señales de voz. Cada canal asignado

a un usuario es de 30 KHz y opera bajo la modalidad simplex. Tanto el receptor como el emisor utilizan la misma frecuencia y por lo general esta tecnología es usada en los sistemas de radio comercial y televisión.

TDMA. El acceso múltiple por división del tiempo (TDMA / Time Division Multiple Access) es el proceso por el cual a un usuario se le asigna una porción de tiempo para su conversación. En sistemas celulares digitales, la información debe ser convertida desde su origen análogo (Voz humana) en datos digitales (1s y 0s). Un dispositivo codificador/decodificador realiza la conversión analógica-a-digital-a-analógica. Entre más eficiente sea este dispositivo, puede asignar más porciones de tiempo para ser compartidas por los usuarios. Por ejemplo, si la voz humana puede ser comprimida a una tasa de 5:1, entonces 5 porciones de tiempo podrían estar disponibles. Por lo general TDMA asigna tres porciones de tiempo en cada canal de 30 KHz.

CDMA. El acceso múltiple por división de código (CDMA / Code Division Multiple Access) es el más eficiente de los sistemas de acceso y está desplazando significativamente los sistemas FDMA y TDMA. En lugar de dividir los usuarios en tiempo o frecuencia cada usuario obtiene todo el espectro de radio en todo momento. Las actuales implementaciones de la técnica CDMA utilizan un ancho de banda de canal de 1.25 MHz comparados con los 30 MHz usados por FDMA y TDMA. Un tamaño de canal de 1.25 MHz permite la propagación de 128 llamadas simultáneas gracias a la codificación digital. Múltiples conversaciones pueden ocurrir sobre el mismo canal y todas se transmiten codificadas en forma digital. Debido al amplio uso de esta tecnología en los sistemas de telefonía celular, las estaciones base poseen toda la infraestructura necesaria para manipular (extraer) las conversaciones individuales codificadas. CDMA cuenta con beneficios muy atractivos como mayor capacidad, mayor seguridad y mejor calidad de las llamadas.

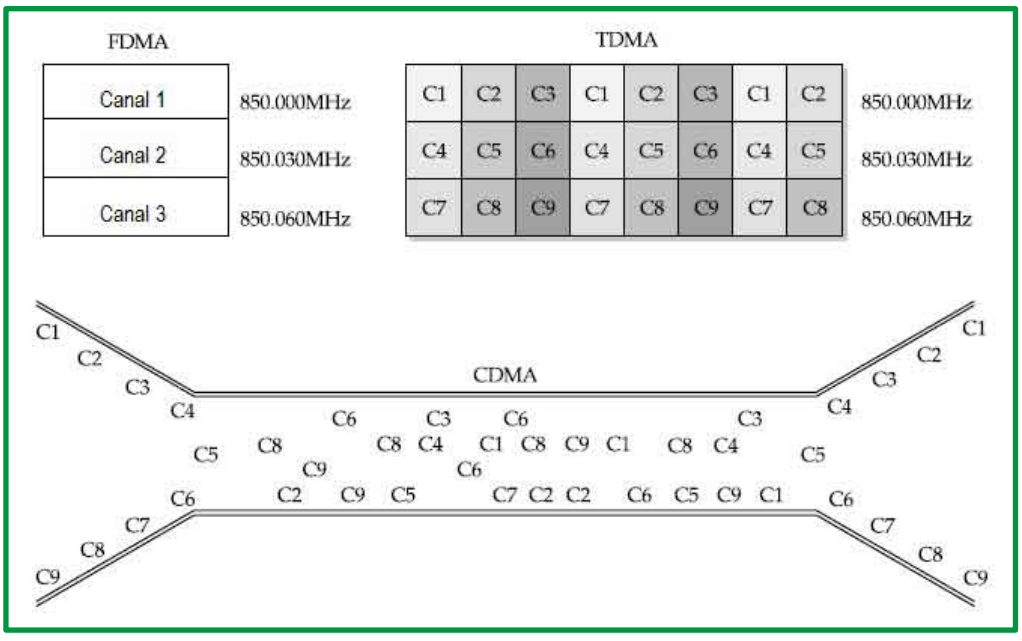


Figure 66: Comparación de técnicas de multiplexación.

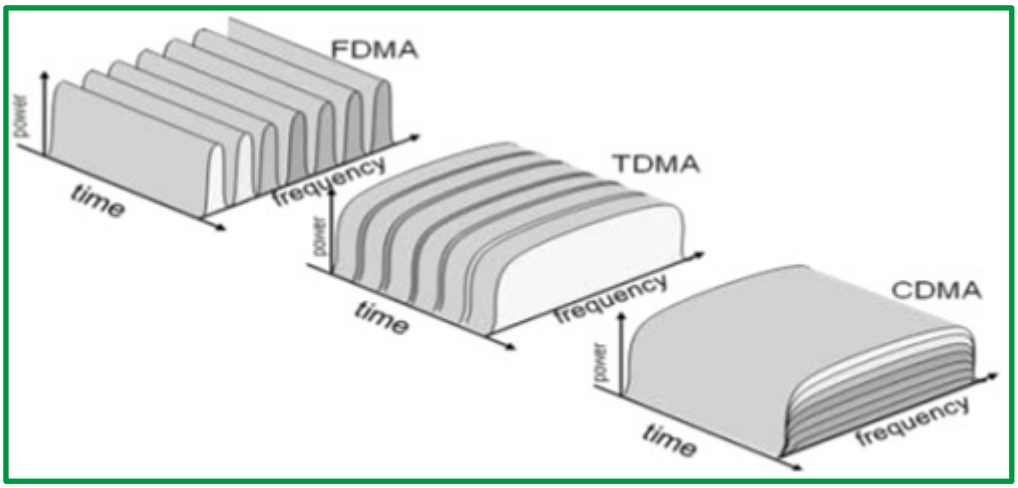


Figure 67: Técnicas de multiplexación.

OFDMA (Acceso Múltiple por División de Frecuencias Ortogonales). Es una técnica basada en la modulación multiportadora (Multi Carrier Modulation MCM) y acceso múltiple por división de frecuencia. La idea básica de la modulación multiportadora es dividir una señal de banda ancha en subportadoras paralelas sin que estas se traslapen.

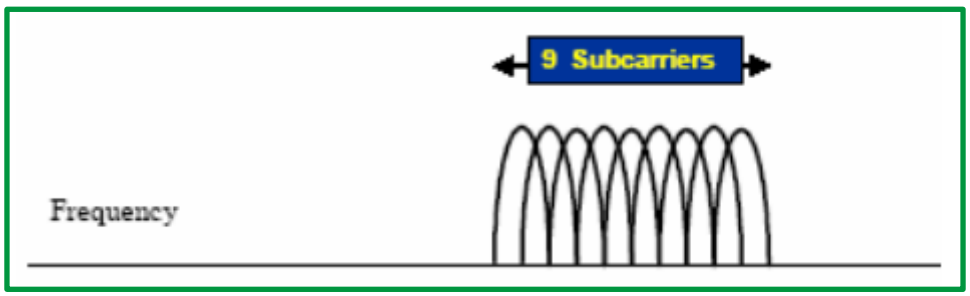


Figure 68: Multiplexado por División de Frecuencias Ortogonales (OFDM).

OFDMA permite que varias subportadoras sean asignadas a diferentes usuarios, así por ejemplo las subportadoras 1, 3 y 7 pueden ser asignadas al ***usuario 1*** y las subportadoras 2, 5 y 9 al ***usuario 2***. Estos grupos de subportadoras son conocidas como subcanales.

OFDMA es similar a FDMA, pero mucho más eficiente espectralmente debido a que el espaciamiento entre subportadoras es reducido, incluso traslapado sin que esto represente pérdida de información. En un sistema que use OFDMA el transmisor y receptor deben de estar sincronizados, esto significa que ambos deben de contar con la misma frecuencia de modulación y la misma escala de tiempo para llevar a cabo la transmisión y poder recuperar la información sin confundirla con la de algún otro usuario.

Multiplexación por división de longitud de onda (WDM)

La multiplexación por división de longitud de onda es una tecnología que permite transmitir varias señales independientes sobre una sola fibra óptica, mediante portadoras ópticas de diferente longitud de onda.

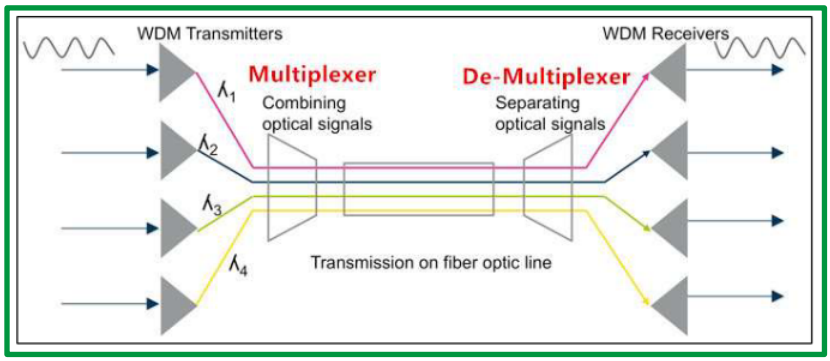


Figure 69: Multiplexación por división de longitud de onda

Los elementos que forman parte del esquema de multiplexación por división de onda son:

- **Dispositivos de transmisión WDM**. Dispositivos con los que los clientes dan inicio a la comunicación, cada uno operando a una longitud de onda diferente.
- **Multiplexor**. Dispositivo de derivación con dos o más puertos de entrada y un puerto de salida, en el que la señal luminosa en cada puerto de entrada se limita a una gama de longitudes de onda previamente seleccionada y la salida es la combinación de las señales luminosas procedentes de los puertos de entrada (UIT-T G.694.1, 2002).
- **Infraestructura física.** Cable de fibra óptica.
- **Demultiplexor de longitud de onda**. Dispositivo que lleva a cabo la operación inversa del multiplexor de longitud de onda, en el que la entrada es una señal óptica que comprende dos o más gamas de longitudes de onda y la salida de cada puerto es una gama de longitudes de onda preseleccionada distinta (UIT-T G.694.1, 2002).
- **Dispositivos de recepción WDM**. Dispositivo en el cliente final que recepta la información original.

Existen varias divisiones de este método WDM, entre lo que están CWDM, DWDM y la más actual UDWDM. La técnica de CWDM multiplexa una menor cantidad de longitudes de onda por canal de fibra óptica. En la técnica DWDM el espaciado entre longitudes de onda es de aproximadamente 1.6nm mientras que en la técnica del CWDM es de 20nm; finalmente la técnica UDWDM trabaja con una amplia gama de longitudes de onda y el espaciamiento entre ellas es de 0.08nm.

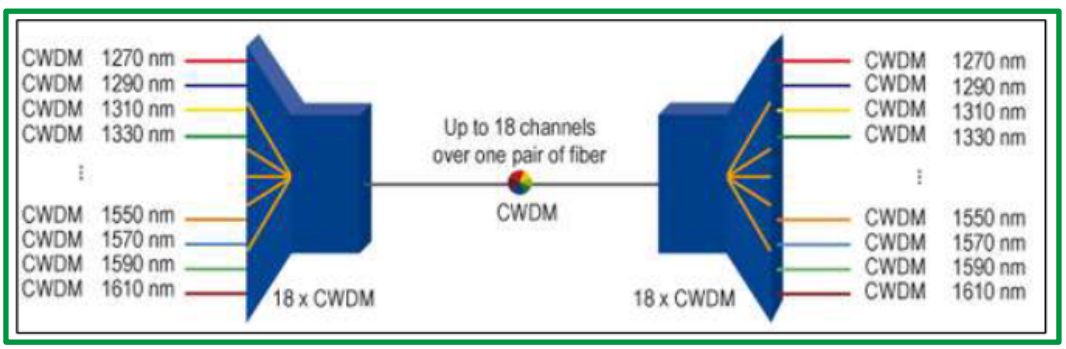


Figure 70: Técnica CWDM

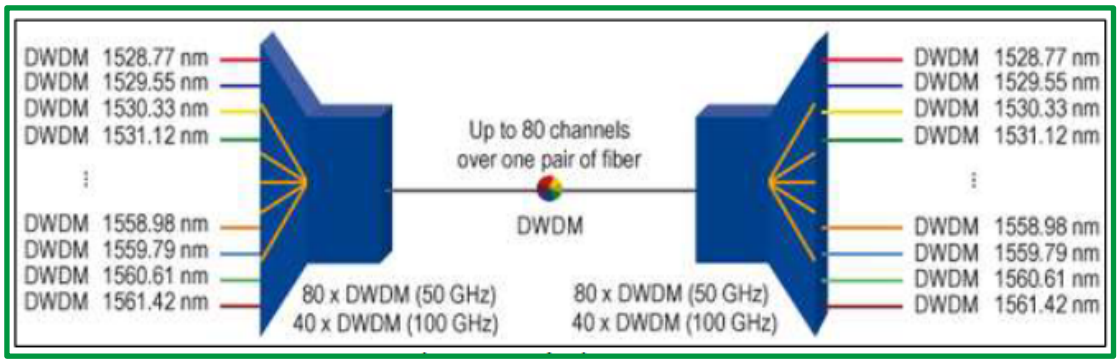


Figure 71: Técnica DWDM

Dominios de colisión y de difusión en medios compartidos.

Dominios de colisión

Al expandir una LAN Ethernet para alojar más usuarios con mayores requisitos de ancho de banda, aumenta la posibilidad de que se produzcan colisiones. Para reducir el número de nodos en un determinado segmento de red, se pueden crear segmentos físicos de red individuales, llamados dominios de colisión.

El área de red donde se originan las tramas y se producen las colisiones se denomina dominio de colisiones. Todos los entornos de los medios compartidos, como aquellos creados mediante el uso de hubs, son dominios de colisión. Cuando un host se conecta a un puerto de switch, el switch crea una conexión dedicada. Esta conexión se considera como un dominio de colisiones individual, dado que el tráfico se mantiene separado de cualquier otro y, por consiguiente, se eliminan las posibilidades de colisión.

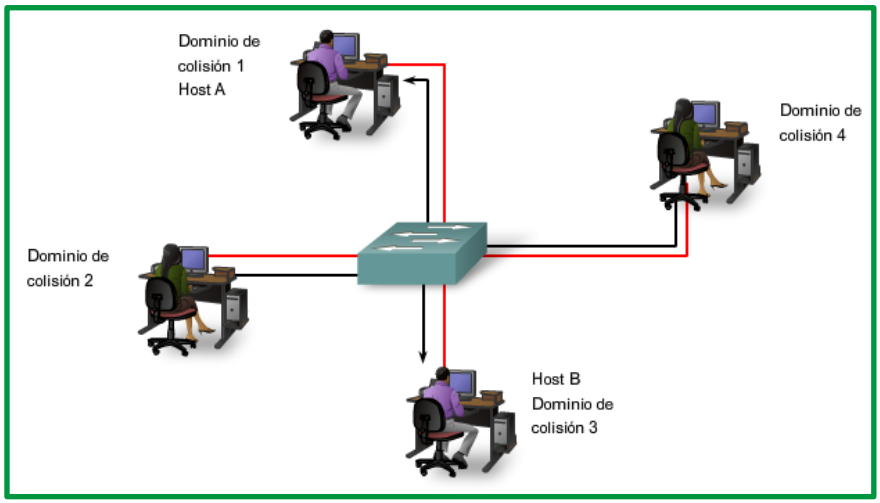


Figure 72: Comunicación hots A - host B

La figura muestra dominios de colisión exclusivos en un entorno conmutado. Por ejemplo: si un switch de 12 puertos tiene un dispositivo conectado a cada puerto, se crean 12 dominios de colisión.

Como se mencionó anteriormente, un switch crea una tabla de direcciones MAC mediante el registro de direcciones MAC de los hosts que están conectados a cada puerto de switch. Cuando dos hosts conectados desean comunicarse entre sí, el switch utiliza la tabla de conmutación para establecer la conexión entre los puertos. El circuito se mantiene hasta que finaliza la sesión.

En la figura, el Host A y el Host B desean comunicarse entre sí. El switch crea la conexión a la que se denomina microsegmento. El microsegmento se comporta como una red de sólo dos hosts, un host que envía y otro que recibe, y se utiliza el máximo ancho de banda disponible.

Los switches reducen las colisiones y permiten una mejor utilización del ancho de banda en los segmentos de red, ya que ofrecen un ancho de banda dedicado para cada segmento de red.

Dominios de broadcast

Si bien los switches filtran la mayoría de las tramas según las direcciones MAC, no hacen lo mismo con las tramas de broadcast. Para que otros switches de la LAN obtengan tramas de broadcast, éstas deben ser reenviadas por switches. Una serie de switches interconectados forma un dominio de broadcast simple. Sólo una entidad de capa 3, como un router o una LAN virtual (VLAN), puede detener un dominio de broadcast de capa 3. Los routers y las VLAN se utilizan para segmentar los dominios de colisión y de broadcast.

Cuando un dispositivo desea enviar un broadcast de capa 2, la dirección MAC destino en la trama se establece en sólo unos. Al configurar el destino en este valor, todos los dispositivos aceptarán y procesarán la trama de broadcast.

El dominio de broadcast de la capa 2 se conoce como dominio de broadcast MAC. El dominio de broadcast MAC incluye todos los dispositivos de la LAN que reciben broadcasts de tramas a través de un host a todas las demás máquinas en la LAN

Cuando un switch recibe una trama de broadcast la reenvía a cada uno de sus puertos excepto al puerto entrante en el que el switch recibió esa trama. Cada dispositivo conectado reconoce la trama de broadcast y la procesa. Esto provoca una disminución en la eficacia de la red dado que el ancho de banda se utiliza para propagar el tráfico de broadcast.

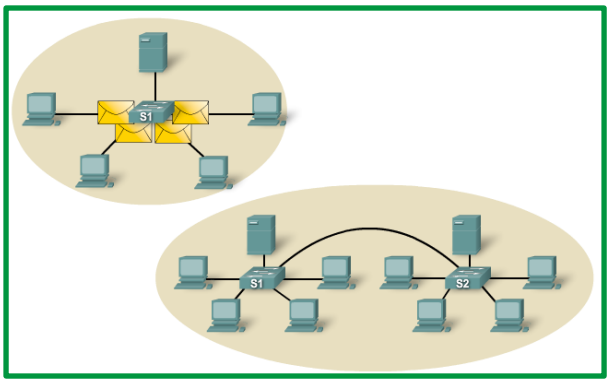


Figure 73: Reenvió de trama broadcast en segmento de red utilizando switch

Cuando se conectan dos switches, el dominio de broadcast aumenta. En la figura anterior, se reenvía una trama de broadcast a todos los puertos conectados en el switch S1. El switch S1 está conectado al switch S2. La trama se propaga a todos los dispositivos conectados al switch S2.

Latencia de red

La latencia es el tiempo que una trama o paquete tarda en hacer el recorrido desde la estación origen hasta su destino final. Los usuarios de las aplicaciones basadas en redes experimentan la latencia cuando tienen que esperar varios minutos para obtener acceso a la información almacenada en un centro de datos o cuando un sitio Web tarda varios minutos en cargar el explorador. La latencia consiste en por lo menos tres componentes.

En primer lugar, ***el tiempo que toma la NIC origen*** en colocar pulsos de voltaje en el cable y el tiempo que tarda la NIC destino en interpretar estos pulsos.

En segundo lugar, ***el retardo de propagación real***, ya que la señal tarda un tiempo en recorrer el cable. Normalmente, éste es de unos 0,556 microsegundos por 100 m para Cat 5 UTP. Si la longitud del cable es mayor y la velocidad nominal de propagación (NVP, Nominal Velocity of Propagation) es menor, el retraso de propagación será mayor.

En tercer lugar, ***la latencia aumenta según los dispositivos de red*** que se encuentren en la ruta entre dos dispositivos. Estos pueden ser dispositivos de capa 1, capa 2 o capa 3.

La latencia no depende únicamente de la distancia y de la cantidad de dispositivos. Por ejemplo: si dos computadoras están separadas por tres switches correctamente configurados, es probable que éstas experimenten una latencia menor que la que se produciría si estuvieran separadas por dos routers correctamente configurados. Esto se debe a que los routers ejecutan funciones más complejas y que llevan más tiempo. Por ejemplo: un router debe analizar datos de capa 3 mientras que los switches sólo analizan los datos de capa 2. Dado que los datos de la capa 2 se presentan antes que los de la capa 3 en la estructura de la trama, los switches pueden procesarla con mayor velocidad. Los switches también admiten alta velocidad de transmisión de voz, video y redes de datos mediante circuitos integrados de aplicaciones específicas (ASIC, Application Specific Integrated Circuits) que proporcionan soporte de hardware para muchas tareas de networking. Otras características de los switches, como por ejemplo búfer de memoria basado en puerto, calidad de servicio (QoS) de nivel de puertos y administración de congestión, también ayudan a reducir la latencia en la red.

La latencia basada en switches puede también deberse a un exceso de demanda en la estructura de éste. Muchos switches de nivel de entrada no cuentan con el rendimiento interno suficiente como para administrar las capacidades del ancho de banda completo en todos los puertos de manera simultánea. El switch debe tener la capacidad de administrar la cantidad máxima de datos que se espera en la red. La causa predominante de latencia de red en una LAN conmutada está más relacionada con los medios que se transmiten, los protocolos de enrutamiento utilizados y los tipos de aplicaciones que se ejecutan en la red.

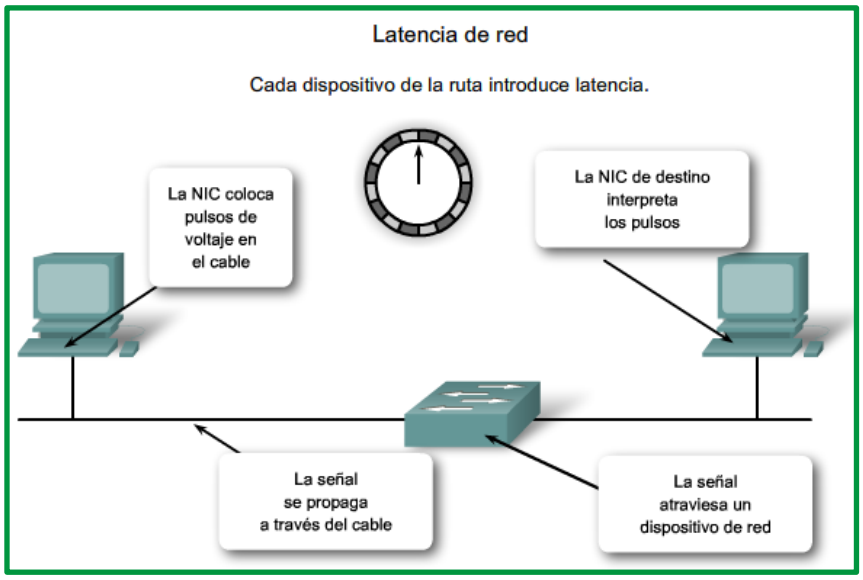


Figure 74: Latencia de red generada principalmente por los medios de transmisión

Segmentación LAN

Las LAN se segmentan en varios dominios de broadcast y de colisión más pequeños mediante el uso de routers y switches. Anteriormente se utilizaban los puentes, pero no suele verse este tipo de equipos de red en una moderna LAN conmutada. La figura muestra los routers y switches que segmentan una LAN.

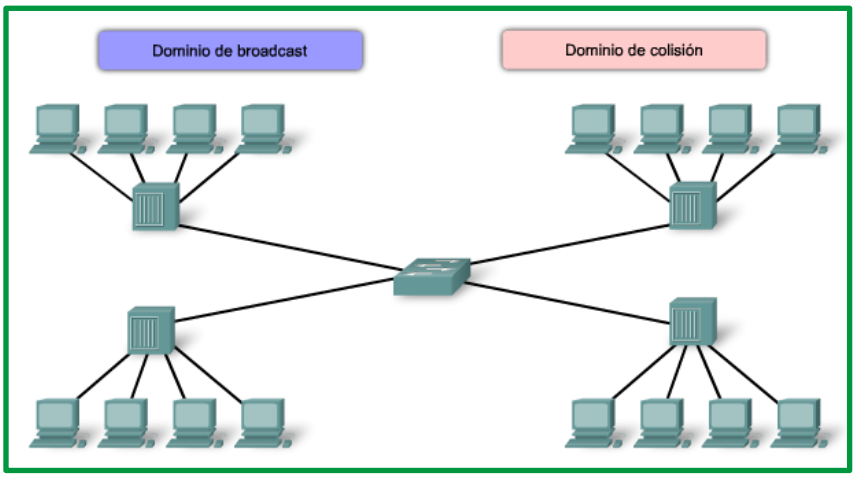


Figure 75 : Dominio sin control de broadcast y dominio de colisión

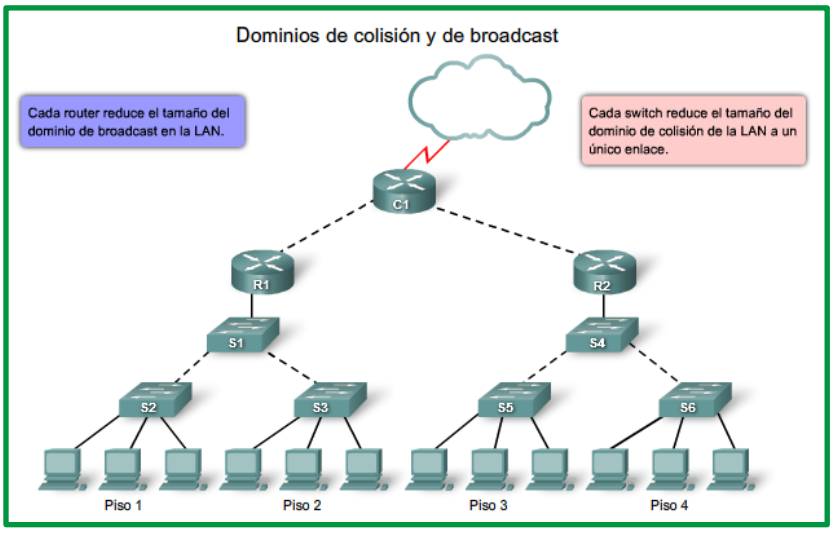


Figure 76: Dominios de colisión y broadcast con control

En la figura, la red está segmentada en dos dominios de colisión mediante el switch.

Puentes y switches

Si bien los puentes y los switches tienen muchos atributos en común, su tecnología presenta varias diferencias. Los puentes se utilizan generalmente para dividir una LAN en un par de segmentos más pequeños. En cambio, los switches se utilizan, por lo general, para dividir una gran LAN en varios segmentos más pequeños. Los puentes tienen sólo un par de puertos para la conectividad de la LAN, mientras que los switches cuentan con varios.

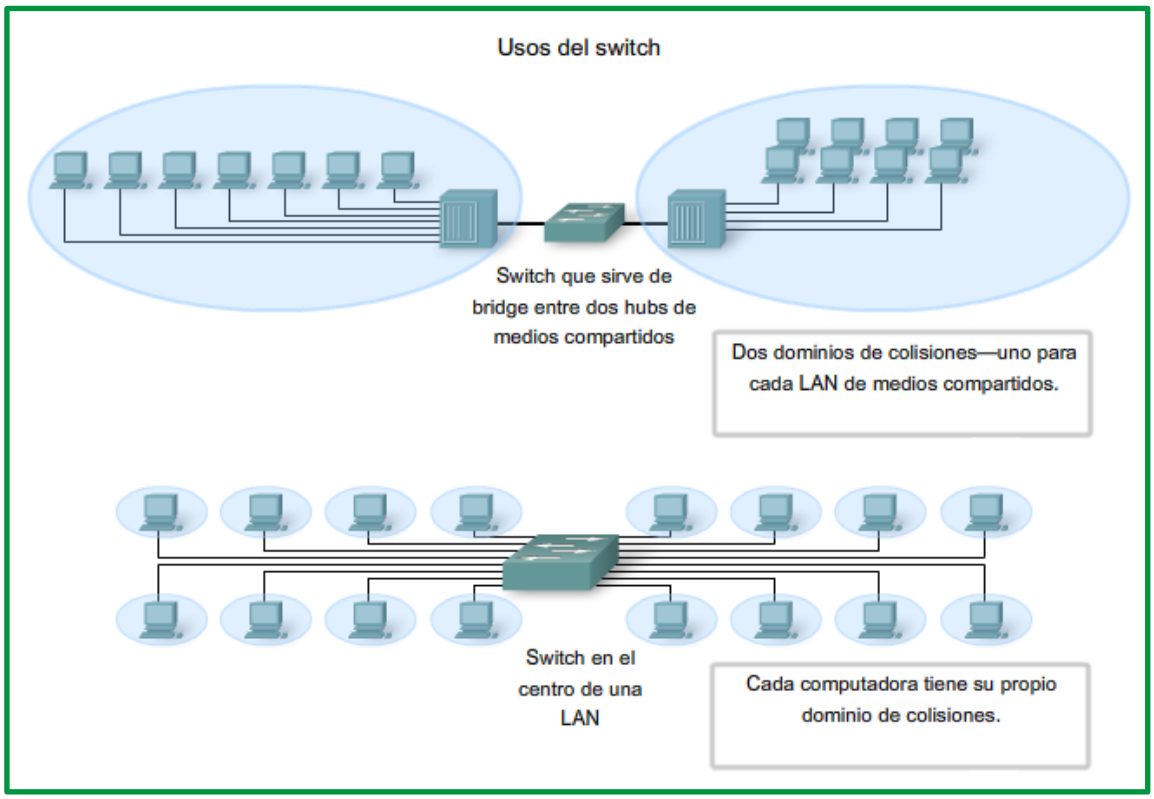


Figure 77: Aplicación de switch en redes LAN para segmentar las redes

Routers

Aunque el switch LAN reduce el tamaño de los dominios de colisión, todos los hosts conectados al switch pertenecen al mismo dominio de broadcast. Los routers pueden utilizarse para crear dominios de broadcast, ya que no reenvían tráfico de broadcast predeterminado. Si se crean pequeños dominios de broadcast adicionales con un router, se reducirá el tráfico de broadcast y se proporcionará mayor disponibilidad de ancho de banda para las comunicaciones unicast. Cada interfaz del router se conecta a una red individual que contiene tráfico de broadcast dentro del segmento de la LAN en el que se originó.

Control de la latencia de la red

Al diseñar una red para reducir la latencia, se necesita tener en cuenta la latencia originada por cada dispositivo de la red. Los switches pueden provocar latencia cuando se saturan en una red ocupada. Por ejemplo: si un switch central tiene que brindar soporte a 48 puertos, siendo cada uno capaz de funcionar a 1000 Mb/s full duplex, el switch tendría que admitir aproximadamente 96 Gb/s de rendimiento interno para mantener la velocidad plena del cable en todos los puertos al mismo tiempo. En este ejemplo, los requisitos de rendimiento mencionados son típicos de los switches de nivel central y no de los switches de nivel de acceso.

El empleo de dispositivos de capas superiores también puede aumentar la latencia en la red. Cuando un dispositivo de capa 3, como un router, debe examinar la información de direccionamiento que contiene la trama, debe realizar una lectura más profunda de la trama que un dispositivo de capa 2, lo cual se traduce en mayor cantidad de tiempo de procesamiento. Al limitar el uso de dispositivos de capas superiores, se reducirá el nivel de latencia de la red. No obstante, la correcta utilización de los dispositivos de capa 3 ayuda a evitar la contención del tráfico de broadcast en un dominio amplio de broadcast o el alto índice de colisiones en un dominio de colisiones de gran tamaño.

Hubs y dominio de colisión

Debido al rápido crecimiento de la Internet:

- Se conectan más dispositivos a la red.
- Los dispositivos acceden a los medios de la red con una mayor frecuencia.
- Aumentan las distancias entre los dispositivos.

Recuerde que los hubs se crearon como dispositivos de red intermediarios que permiten a una mayor cantidad de nodos conectarse a los medios compartidos. Los hubs, que también se conocen como repetidores multipuerto, retransmiten las señales de datos recibidas a todos los dispositivos conectados, excepto a aquél desde el cual se reciben las señales. Los hubs no desempeñan funciones de red tales como dirigir los datos según las direcciones. Los hubs y los repetidores son dispositivos intermediarios que extienden la distancia que pueden alcanzar los cables de Ethernet. Debido a que los hubs operan en la capa física, ocupándose únicamente de las señales en los medios, pueden producirse colisiones entre los dispositivos

que conectan y dentro de los mismos hubs. Además, el uso de hubs para proporcionar acceso a la red a una mayor cantidad de usuarios reduce el rendimiento para cada usuario, ya que debe compartirse la capacidad fija de los medios entre cada vez más dispositivos.

Los dispositivos conectados que tienen acceso a medios comunes a través de un hub o una serie de hubs conectados directamente conforman lo que se denomina dominio de colisiones. Un dominio de colisiones también se denomina segmento de red. Por lo tanto, los hubs y los repetidores tienen el efecto de aumentar el tamaño del dominio de colisiones. Como se muestra en la siguiente figura, la interconexión de los hubs forma una topología física que se denomina estrella extendida. La estrella extendida puede crear un dominio de colisiones notablemente expandido.

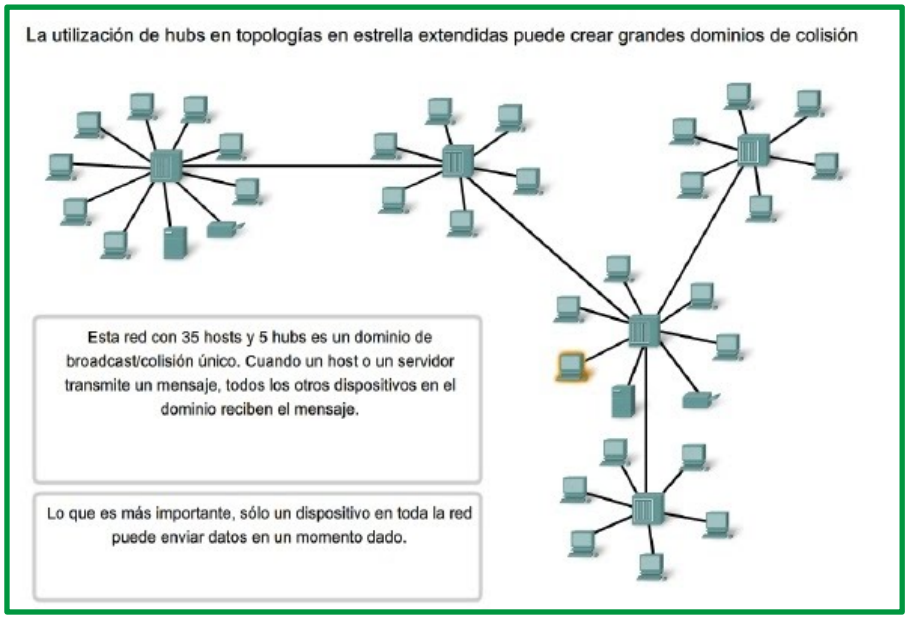


Figure 78: Ejemplo de un dominio de colisión

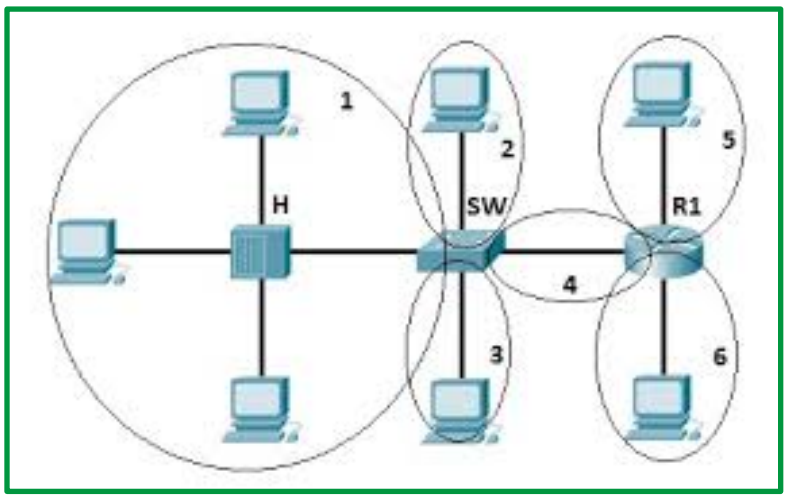


Figure 79: Dominios de colisión y de broadcast

Detección y corrección de errores

Las redes deben ser capaces de transferir datos de un dispositivo a otro con total exactitud, si los datos recibidos no son idénticos a los emitidos, el sistema de comunicación es inútil. Sin embargo, siempre que se transmiten de un origen a un destino, se pueden corromper por el camino. Los sistemas de comunicación deben tener mecanismos para detectar y corregir errores que alteren los datos recibidos debido a múltiples factores de la transmisión.

La detección y corrección de errores se implementa bien en el nivel de enlace de datos o bien en el nivel de transporte del modelo OSI.

Tipo de errores

Las propiedades físicas y los fenómenos de los medios pueden generar interferencias, calor, magnetismo, etc, que influyen en una señal electromagnética, esos factores pueden alterar la forma o temporalidad de una señal. Si la señal transporta datos digitales, los cambios pueden modificar el significado de los datos. Los errores posibles son:

- **Error de bit**. Únicamente un bit de una unidad de datos determinada cambia de 1 a 0 o viceversa.

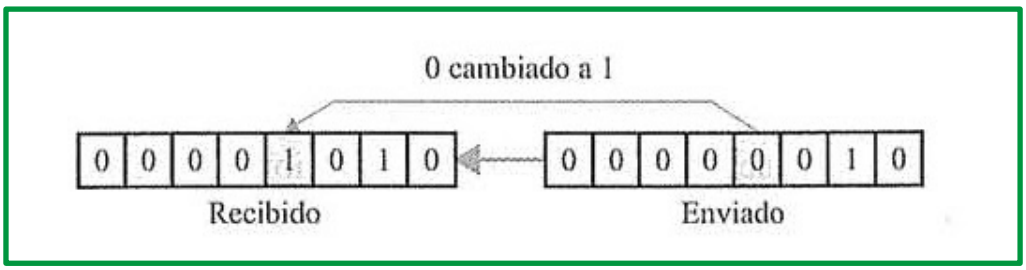


Figure 80: Error de bit

  Un error de bit altera el significado del dato. Son el tipo de error menos probable en una transmisión de dato serial, puesto que el intervalo de bit es muy breve (1/frecuencia) el ruido tiene que tener una duración muy breve. Sin embargo, si puede ocurrir en una transmisión paralela, en que un cable puede sufrir una perturbación y alterar un bit de cada byte.

- **Error de ráfaga**. El error de ráfaga significa que dos o más bits de la unidad de datos han cambiado. Los errores de ráfaga no significan necesariamente que los errores se produzcan en bits consecutivos. La longitud de la ráfaga se mide desde el primero hasta el último bit correcto, algunos bits intermedios pueden estar correcto.

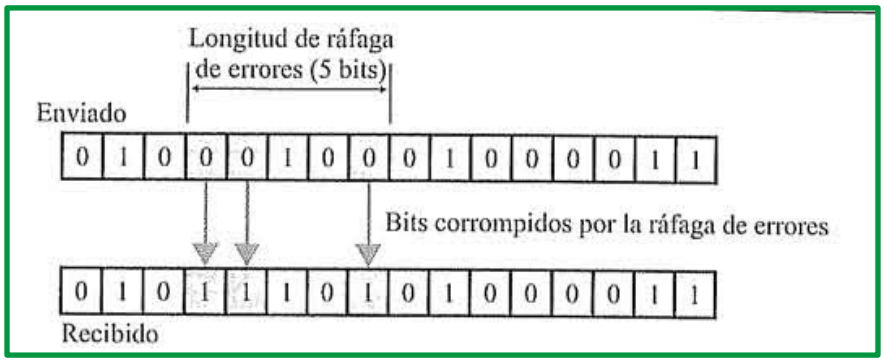


Figure 81: Error de ráfaga

Los errores de ráfaga son más probables en transmisiones serie, donde la duración del ruido es normalmente mayor que la duración de un bit, por lo que afectara a un conjunto de bits. El número de bits afectados depende de la tasa de datos y de la duración del ruido.

Error de desvanecimiento.

Método de detección de errores

Verificación de paridad

La verificación de paridad (a veces denominada VRC o verificación de redundancia vertical) es uno de los mecanismos de verificación más simples. Consiste en agregar un bit adicional (denominado bit de paridad) a un cierto número de bits de datos denominado palabra código (generalmente 7 bits, de manera que se forme un byte cuando se combina con el bit de paridad) cuyo valor (0 o 1) es tal que el número total de bits 1 es par. Para ser más claro, 1 si el número de bits en la palabra código es impar, 0 en caso contrario. Tomemos el siguiente ejemplo:

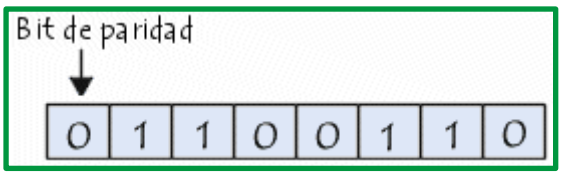


Figure 82: Ejemplo bit de paridad

En este ejemplo, el número de bits de datos 1 es par, por lo tanto, el bit de paridad se determina en 0. Por el contrario, en el ejemplo que sigue, los bits de datos son impares, por lo que el bit de paridad se convierte en 1.

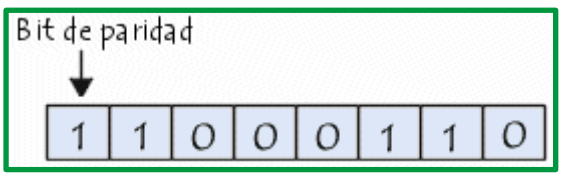


Figure 83: Ejemplo bit de paridad

Supongamos que después de haber realizado la transmisión, el bit con menos peso del byte anterior (aquel que se encuentra más a la derecha) ha sido víctima de una interferencia:

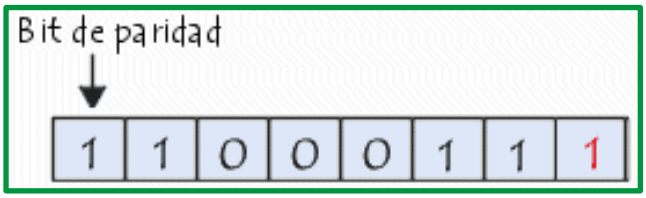


Figure 84: Ejemplo bit de paridad

El bit de paridad, en este caso, ya no corresponde al byte de paridad: se ha detectado un error. Sin embargo, si dos bits (o un número par de bits) cambian simultáneamente mientras se está enviando la señal, no se habría detectado ningún error.

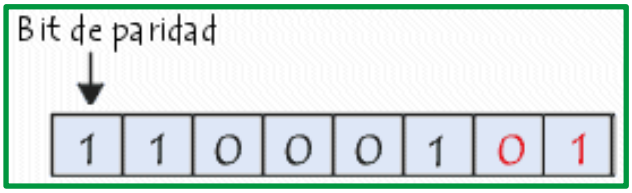


Figure 85: Ejemplo bit de paridad

Ya que el sistema de control de paridad puede detectar un número impar de errores, puede detectar solamente el 50% de todos los errores. Este mecanismo de detección de errores también tiene la gran desventaja de ser incapaz de corregir los errores que encuentra (la única forma de arreglarlo es solicitar que el byte erróneo sea retransmitido).

Verificación de redundancia longitudinal

La verificación de la redundancia longitudinal (LRC, también denominada verificación de redundancia horizontal) no consiste en verificar la integridad de los datos mediante la representación de un carácter individual, sino en verificar la integridad del bit de paridad de un grupo de caracteres.

Digamos que "HELLO" es el mensaje que transmitiremos utilizando el estándar ASCII. Estos son los datos tal como se transmitirán con los códigos de verificación de redundancia longitudinal:

Letra	Código ASCII (7 bits)	Bit de paridad (LRC)
H	1001000	0
E	1000101	1
L	1001100	1
L	1001100	1
0	1001111	1
VRC	1000010	0

Figure 86: Ejemplo LRC

Verificación de redundancia cíclica

La verificación de redundancia cíclica (abreviado, CRC) es un método de control de integridad de datos de fácil implementación. Es el principal método de detección de errores utilizado en las telecomunicaciones.

La verificación de redundancia cíclica consiste en la protección de los datos en bloques, denominados tramas. A cada trama se le asigna un segmento de datos denominado código de control (al que se denomina a veces FCS, secuencia de verificación de trama, en el caso de una secuencia de 32 bits, y que en ocasiones se identifica erróneamente como CRC). El código CRC contiene datos redundantes con la trama, de manera que los errores no sólo se pueden detectar, sino que además se pueden solucionar.

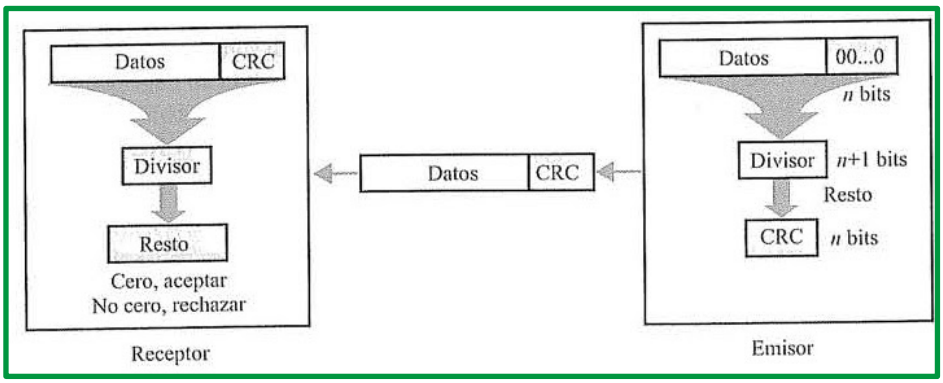


Figure 87: Esquema del proceso CRC

Sumas de comprobación. Es el método de detección usado por los protocolos de alto nivel, se basa en el concepto de redundancia.

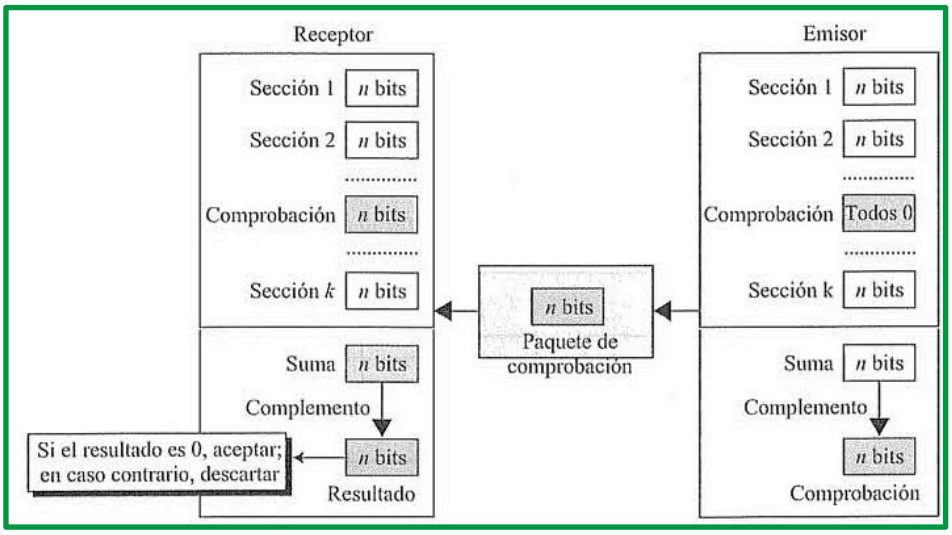


Figure 88: Proceso de suma de comprobación.

- **Generador de suma de comprobación**.

En el emisor, el generador subdivide la unidad de datos en segmentos iguales de n bits (habitualmente n=16), estos segmentos se suman usando una aritmética de

complemento a uno, de forma que la suma sea también n bits, a continuación, se complementa la suma y ese dato complementado se añade al final de la unidad de datos original como bits de redundancia, la unidad extendida se transmite por la red.

- **Comprobador de suma de comprobación**.

El receptor subdivide las unidades de datos en los mismos n bits, suma todos los segmentos (incluidos los bits de redundancia) y luego complementa el resultado, si la unidad de datos está intacta, el valor final que se obtiene es nulo (n bits 0), si en resultado no es cero, el paquete contiene un error y es rechazado.

Método de corrección de errores

En toda transmisión digital sobre un canal real los niveles eléctricos de la señal están expuestos a pequeñas variaciones ocasionadas por interferencias, ruido o el incorrecto funcionamiento de alguno de los equipos que componen el canal. La suma de estos factores puede llegar a cambiar la interpretación de los bits alterando el significado de la información enviada.

En un canal la calidad de este se mide en base a la tasa de error BER (Bit Error Rate) que se obtiene como el resultado de medir el número de bit recibidos erróneos entre el total de bit transmitidos.

BER = nº de bit recibidos erróneos/total de bit transmitidos.

Existen multitud de protocolos de detección y corrección de errores que establecen un conjunto de normas para sincronizar y ordenar las tramas de datos y definen procedimientos para determinar cuándo se ha producido un error y como deben corregirse. Entre los métodos más usados para corregir errores en transmisiones digitales destacan:

- Sustitución de símbolos.
- Retransmisión (ARQ).
- Corrección de errores en sentido directo o hacia adelante (FEC).

Sustitución de símbolos

Se diseñó para utilizarse cuando haya un ser humano en la terminal de recepción. Analiza los datos recibidos y toma decisiones sobre su integridad. En la sustitución de símbolos si se recibe un carácter presuntamente equivocado se sustituye por un carácter que exige al operador que lo vuelva a interpretar. Ejemplo:

Si el mensaje “documento” tuviera un error en el primer carácter, se sustituye la "d" por "%" y se le muestra al operador el mensaje “%ocumento”. En este caso por contexto se puede recuperar el contenido de ese carácter y es innecesaria la retransmisión, pero si el mensaje fuera “&%,000.00” el operador no puede definir cuál es el carácter equivocado y se pide la retransmisión del mensaje.

Retransmisión

Cuando no se está operando en tiempo real puede ser útil pedir el reenvío íntegro de las tramas que se presumen erróneas o dañadas. Éste es posiblemente el método más seguro de corrección de errores, aunque raramente es el método más eficiente.

Es el caso por ejemplo del protocolo ARQ (Automatic Repeat-reQuest) donde el terminal que detecta un error de recepción pide la repetición automática de todo el mensaje.

Si se usan mensajes cortos será menor la probabilidad de que haya una irregularidad en la transmisión, pero sin embargo estos requieren más reconocimientos y cambios de dirección de línea que los mensajes largos. Con los mensajes largos se necesita menos tiempo de cambio de línea, aunque aumenta la probabilidad de que haya un error de transmisión, respecto a los mensajes cortos.

Corrección de errores en sentido directo

Conocido también como FEC (forward error correction) y es el único esquema de corrección de errores que detecta y corrige los errores de transmisión en la recepción, sin pedir la retransmisión del mensaje enviado.

En el sistema FEC se agregan bits al mensaje antes de transmitirlo. Uno de los códigos más difundidos para enviar mensajes es el código Hamming. Donde la cantidad de bits en este código depende de la cantidad de bits en el carácter de datos. Como se observe en la siguiente ecuación: 2^n>m+n+1 y 2^n=m+n+1

Dónde:

n = cantidad de bits de Hamming.

m = cantidad de bits en el carácter de datos.

Código Hamming

En 1950 R. W. Haming, de los Laboratorios Bell, comenzó a utilizar el concepto de distancia, que se define como el número de posiciones en las que dos dígitos binarios de igual longitud defieren. Por ejemplo, en 10010 y 01011 la distancia de Hamming es 3, pues difieren en 3 de las 5 posiciones.

La idea entonces fue establecer un set de caracteres en el que todos tienen entre sí la misma distancia de Hamming, luego en el extremo receptor se verifica cada carácter recibido para determinar si es uno de los caracteres válidos, si no lo es se busca el carácter que tenga la menor distancia de Hamming con este y se le asigna ese valor como “correcto”. Un código de Hamming de distancia 3 puede detectar errores dobles y corregir los simples (de un solo bit). En el caso de errores dobles la “corrección” es errónea ya que como no se sabe si el error es simple o doble se presupone simple y como tal se corrige.

Los códigos de Hamming a propuesta de este se mejoraron agregando a los bits de información una serie de bits de comprobación, a partir de estos últimos se puede detectar la posición de bits erróneos y corregirlos.

Como ejemplo veremos uno de estos códigos de Hamming. Supongamos que tenemos una palabra de información de 8 bits, D1 a D8, agregamos a ella cuatro bits de comprobación, C1 a C4 con la siguiente estructura:

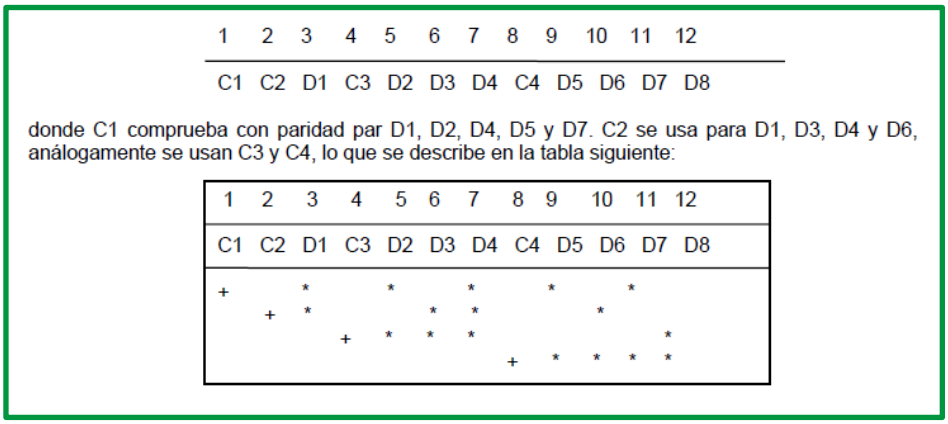


Figure 89: Ejemplo aplicación de código Hamming

Cuando se envían los datos se calculan C1, C2, C3 y C4 y se van comparando los valores recibidos empezando con C4 y terminando con C1, si los valores recibidos y los calculados coinciden se asigna a la comprobación el valor 0 y si difieren se asigna 1. Si todas las comprobaciones dan resultado positivo tendremos un valor 0000 para la secuencia de comprobación. Pero si ha habido un error alguna de las comprobaciones fallará. Supongamos que se ha producido un error en D3, al realizar las comprobaciones de paridad C1 y C4 darán 0 mientras que C2 y C3 darán 1, tendremos una secuencia de comprobación 0110 que representa en binario 6 que es la posición de D3 el bit erróneo; solo queda corregirlo.

El número de bits de comprobación necesaria depende de la longitud de la palabra a transmitir y aunque su funcionamiento parezca engorroso puede implementarse con "hardware" no muy costoso.

Protocolos y tecnologías de enlace de datos

Específicamente, los servicios y las especificaciones de la capa de enlace de datos se definen mediante varios estándares basados en diversas tecnologías y medios a los cuales se aplican los protocolos. Algunos de estos estándares integran los servicios de la Capa 2 y la Capa 1.

Organismo de estandarización	Estándares de red
IEEE	• 802.2: Control de enlace lógico (LLC) • 802.3: Ethernet • 802.4: Token bus • 802.5: Token Ring • 802.11: LAN inalámbrica (WLAN) y malla (certificación Wi-Fi) • 802.15: Bluetooth • 802.16: WiMax
ITU-T	• G.992: ADSL • G.8100 - G.8199: aspectos de MPLS de transporte • Q.921: ISDN • Q.922: Frame Relay
ISO	• Control de enlace de datos de alto nivel (HDLC) • ISO 9314: Control de acceso al medio (MAC) de la FDDI
ANSI	• X3T9.5 y X3T12: Interfaz de datos

Figure 90: Organismo de estandarización y estándar de red de la capa de enlace de datos

La capa de enlace de datos proporciona tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa se ocupa del direccionamiento físico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo. Una trama por lo más general que sea, incluye:

- **Datos**: El paquete desde la Capa de red que contiene el cuerpo del mensaje encapsulado.
- **Encabezado**: Contiene información de control como direccionamiento y está ubicado al comienzo de la trama.
- **Tráiler**: Contiene información de control agregada al final de la trama.

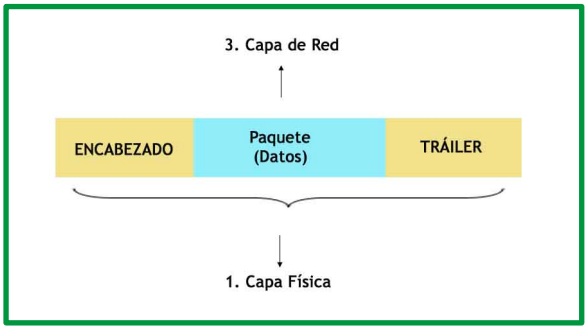


Figure 91: trama capa enlace de datos

Cuando los datos viajan por los medios, se convierten en un stream de bits, o en 1 y 0. Si un nodo terminal está recibiendo streams de bits largos ¿cómo determina dónde comienza y termina la trama o qué bits representan una dirección?

El tramado rompe el stream en agrupaciones descifrables, con la información de control insertada en el encabezado y tráiler como valores en campos diferentes. Este formato brinda a las señales físicas una estructura que puede ser recibida por los nodos y decodificada en paquetes en el destino.

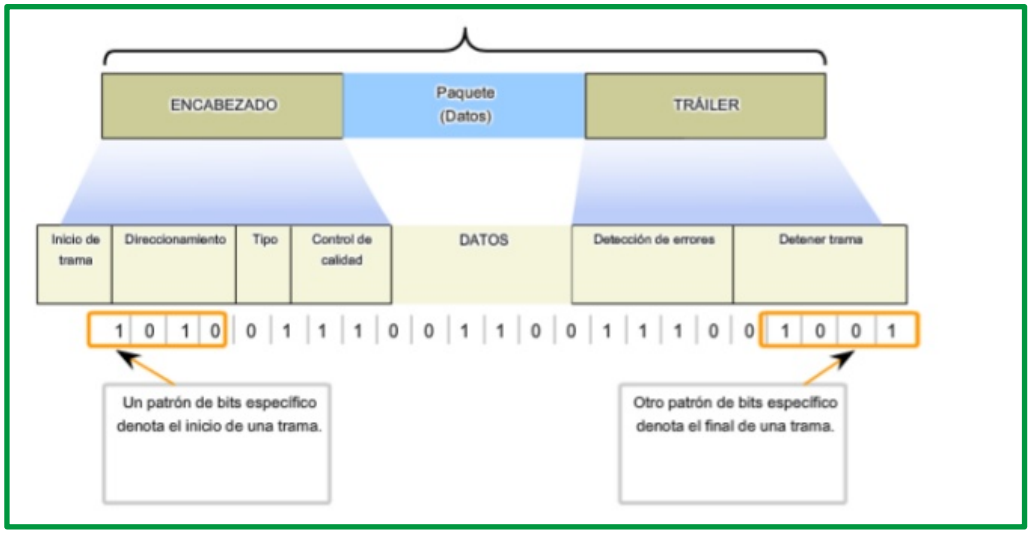


Figure 92:Formateo de los datos para la transmisión.

Los tipos de campos típicos incluyen:

- Campos indicadores de **comienzo** y **detención**: Límites de comienzo y finalización de la trama.
- **Direccionamiento**
- **Campo tipo**: el tipo de PDU contenido en la trama
- **Calidad**: campos de control
- **Campo de datos**: carga de tramas (Paquete de capa de red)
- Campos en el extremo final de la trama desde el tráiler. Estos campos se utilizan para la **detección de errores** y marcan el final de la trama.

No todos los protocolos incluyen todos estos campos. Los estándares para un protocolo de enlace de datos definen el formato real de la trama.

La capa de enlace de datos existe como una capa de conexión entre los procesos de software de las capas por encima de ella y la capa física debajo de ella. Como tal, prepara los paquetes de capa de red para la transmisión a través de alguna forma de medio, ya sea cobre, fibra o entornos /medios inalámbricos.

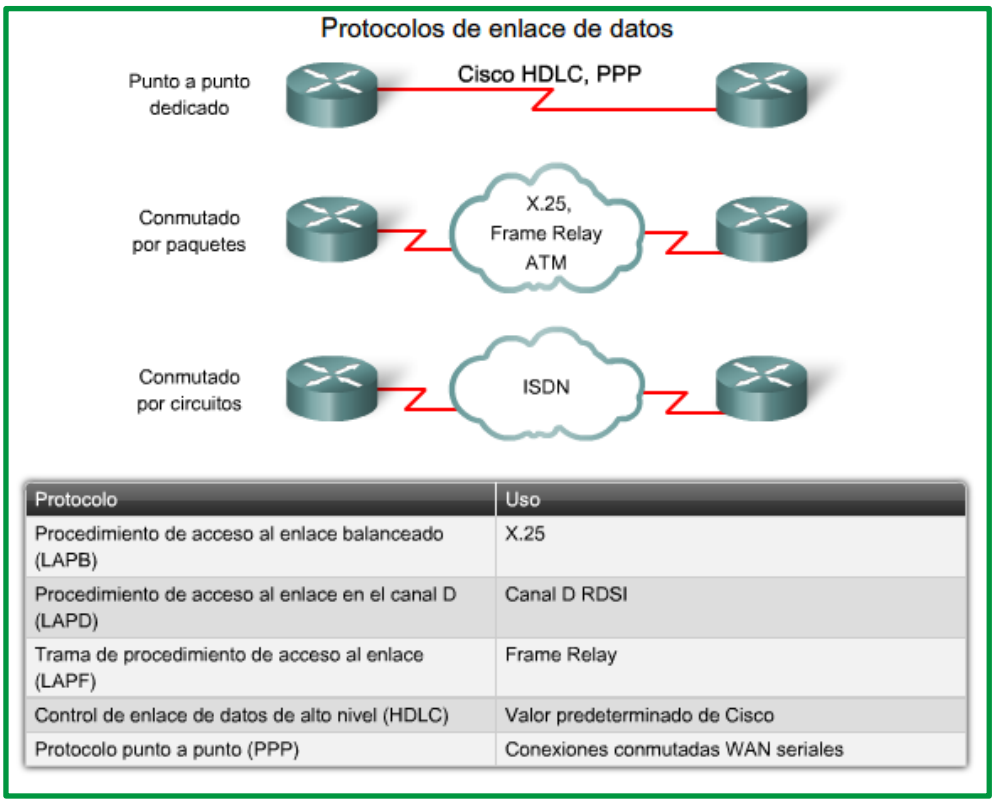
En muchos casos, la Capa de enlace de datos está incorporada en una entidad física como tarjeta de interfaz de red (NIC) de Ethernet, que se inserta dentro del bus del sistema de una computadora, switch o router y hace la conexión entre los procesos de software que se

ejecutan en los dispositivos finales y los medios físicos. Sin embargo, la NIC no es solamente una entidad física. El software asociado con la NIC permite que la NIC realice sus funciones de intermediara preparando los datos para la transmisión y codificando los datos como señales que deben enviarse sobre los medios asociados.

Las WAN necesitan protocolos de la capa de enlace de datos para establecer el vínculo a través de la línea de comunicación, desde el dispositivo emisor hasta el dispositivo receptor.

Los protocolos de la capa de enlace de datos definen cómo se encapsulan los datos para su transmisión a lugares remotos, así como también los mecanismos de transferencia de las tramas resultantes. Se utiliza una variedad de tecnologías diferentes, como ISDN, Frame Relay o ATM. Muchos de estos protocolos utilizan los mismos mecanismos básicos de entramado, HDLC, un estándar ISO o uno de sus subgrupos o variantes. ATM se diferencia de los demás porque utiliza celdas pequeñas de un tamaño fijo de 53 bytes (48 bytes para datos), mientras que las demás tecnologías de conmutación de paquetes utilizan paquetes de tamaño variable. Los protocolos de enlace de datos WAN más comunes son:

- HDLC
- PPP
- Frame Relay
- ATM
- MPLS
- ADSL



Protocolo	Uso
Procedimiento de acceso al enlace balanceado (LAPB)	X.25
Procedimiento de acceso al enlace en el canal D (LAPD)	Canal D RDSI
Trama de procedimiento de acceso al enlace (LAPF)	Frame Relay
Control de enlace de datos de alto nivel (HDLC)	Valor predeterminado de Cisco
Protocolo punto a punto (PPP)	Conexiones conmutadas WAN seriales

Figure 93:Protocolo de enlace de datos

ISDN y X.25 son protocolos de enlace de datos más antiguos que en la actualidad se utilizan con menor frecuencia. Sin embargo, ISDN se utiliza para proporcionar redes VoIP con enlaces PRI. X.25 se menciona para ayudar a explicar la importancia de Frame Relay. Además, X.25 se sigue utilizando en los países en vías de desarrollo, donde se usan redes de datos de paquetes (PDN, packet data network) para transmitir transacciones de tarjetas de crédito y tarjetas de débito de tiendas minoristas.

Otro protocolo de capa de enlace de datos es el protocolo de conmutación de etiquetas multiprotocolos (MPLS, Multiprotocol Label Switching). Los proveedores de servicios están implementando MPLS con mayor frecuencia para proporcionar una solución económica para transportar tráfico de redes de conmutación de circuitos y de conmutación por paquetes. Puede operar a través de cualquier infraestructura existente, por ejemplo, IP, Frame Relay, ATM o Ethernet. Se sitúa entre la Capa 2 y la Capa 3.

X.25

X.25 es un protocolo de capa de red heredado que proporciona una dirección de red a los suscriptores. Los circuitos virtuales se establecen a través de la red con paquetes de petición de llamadas a la dirección destino. Un número de canal identifica la SVC resultante. Los paquetes de datos rotulados con el número del canal se envían a la dirección correspondiente. Varios canales pueden estar activos en una sola conexión.

Las aplicaciones típicas de X.25 son los lectores de tarjeta de punto de venta. Estos lectores utilizan X.25 en el modo de conexión telefónica para validar las transacciones en una computadora central. Para estas aplicaciones, el ancho de banda bajo y la latencia alta no constituyen un problema, y el costo bajo hace que X.25 sea accesible.

Las velocidades de los enlaces X.25 varían de 2400 bps a 2 Mbps. Sin embargo, las redes públicas normalmente tienen una capacidad baja con velocidades que rara vez superan los 64 kbps.

En la actualidad, las redes X.25 están en franca decadencia y están siendo reemplazadas por tecnologías más recientes de capa 2, como Frame Relay, ATM y ADSL. Sin embargo, se siguen utilizando en muchos países en vías de desarrollo, en donde el acceso a las tecnologías más recientes es limitado.

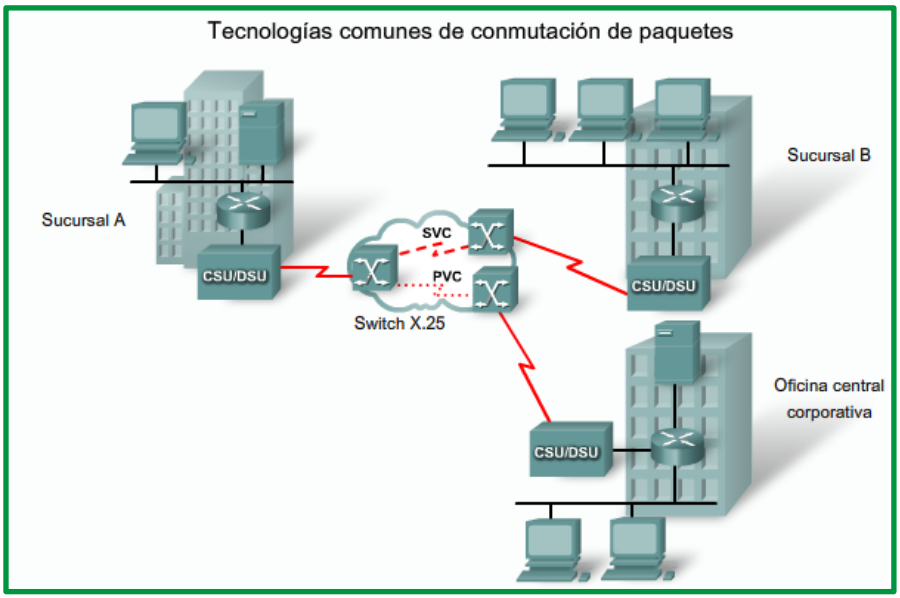


Figure 94: Tecnología X.25

Frame Relay

Si bien el diseño de la red parece ser similar al de las redes X.25, Frame Relay se diferencia de X.25 en varios aspectos. El más importante es que es un protocolo mucho más sencillo que funciona a nivel de la capa de enlace de datos y no en la capa de red. Frame Relay no realiza ningún control de errores o flujo. El resultado de la administración simplificada de las tramas es una reducción en la latencia y las medidas tomadas para evitar la acumulación de tramas en los switches intermedios ayudan a reducir las fluctuaciones de fase. Frame Relay ofrece velocidades de datos de varios Mbps.

Los VC de Frame Relay se identifican de manera única con un DLCI, lo que garantiza una comunicación bidireccional de un dispositivo DTE al otro. La mayoría de las conexiones de Frame Relay son PVC y no SVC.

Frame Relay ofrece una conectividad permanente, compartida, de ancho de banda mediano, que envía tanto tráfico de voz como de datos. Frame Relay es ideal para conectar las LAN de una empresa. El router de la LAN necesita sólo una interfaz, aun cuando se estén usando varios VC. La línea alquilada corta que va al extremo de la red Frame Relay permite que las conexiones sean económicas entre LAN muy dispersas.

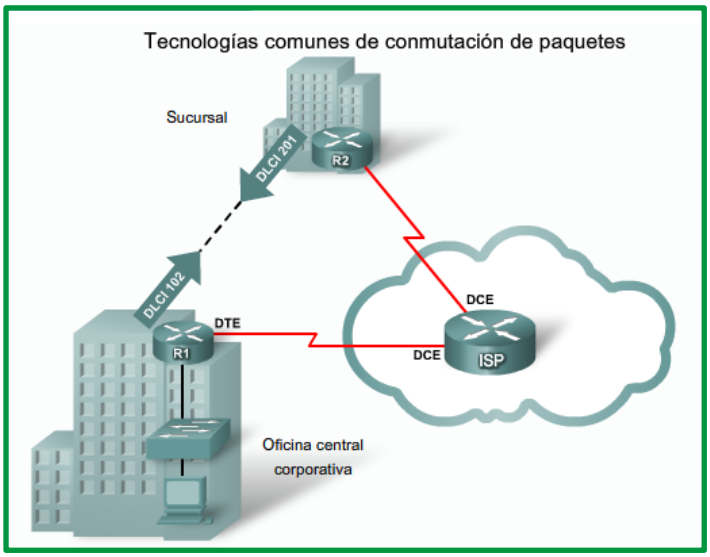


Figure 95:Tecnología Frame Relay

ATM

Modo de transferencia asíncrona (ATM, Asynchronous Transfer Mode) es capaz de transferir voz, video y datos a través de redes privadas y públicas. Tiene una arquitectura basada en celdas, en lugar de tramas. Las celdas ATM tienen siempre una longitud fija de 53 bytes. La celda ATM contiene un encabezado ATM de 5 bytes seguido de 48 bytes de contenido ATM. Las celdas pequeñas de longitud fija son adecuadas para la transmisión de tráfico de voz y video porque este tráfico no tolera demoras. El tráfico de video y voz no tiene que esperar a que se transmita un paquete de datos más grande.

La celda ATM de 53 bytes es menos eficiente que las tramas y paquetes más grandes de Frame Relay y X.25. Además, la celda ATM tiene una carga general de por lo menos 5 bytes por cada 48 bytes de contenido. Cuando la celda está transportando paquetes de capa de red segmentados, la carga general es mayor porque el switch ATM tiene que poder reagrupar los paquetes en el destino. Una línea ATM típica necesita casi un 20 por ciento más de ancho de banda que Frame Relay para transportar el mismo volumen de datos de capa de red.

ATM fue diseñado para ser extremadamente escalable y soporta velocidades de enlace desde T1/E1 hasta OC-12 (622 Mbps) y superiores.

ATM ofrece tanto los PVC como los SVC, aunque los PVC son más comunes en las WAN. Además, como otras tecnologías compartidas, ATM permite varios VC en una sola conexión de línea arrendada al extremo de red.

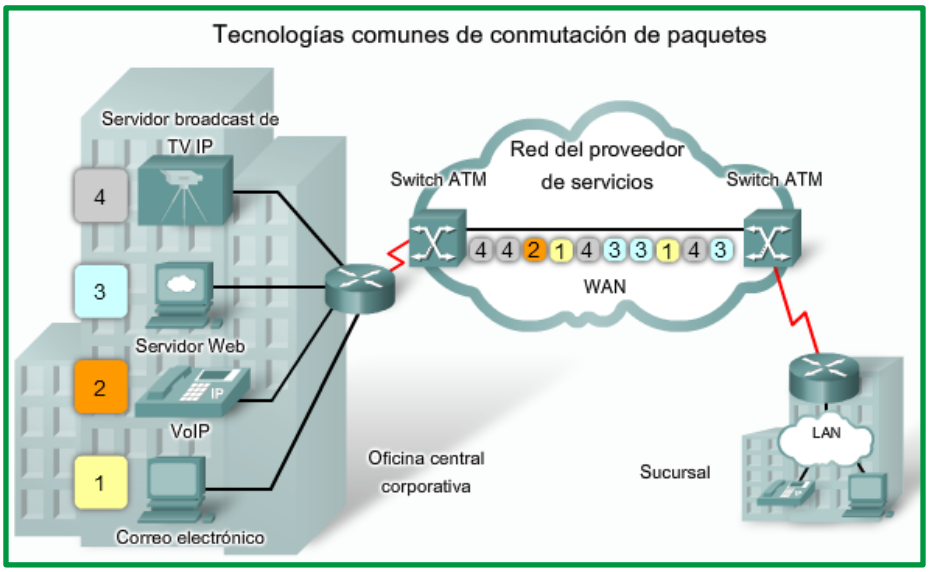


Figure 96: Tecnología ATM

Protocolo de Internet de línea serial (SLIP).

Es un protocolo estándar para conexiones seriales punto a punto mediante TCP/IP. PPP reemplazó ampliamente al protocolo SLIP**.**

MPLS.

Es una tecnología de conmutación de etiquetas que reenvía paquetes en la capa 2, habitualmente dentro de la red de un proveedor de servicios, sin recurrir al enrutamiento de capa 3. Según la definición de IETF RFC 3031, MPLS añade una etiqueta de cuatro bytes a un encabezado de paquetes IP cuando entra en la red MPLS; la etiqueta determina la ruta de reenvío del flujo de tráfico sin necesidad de saltos intermedios para inspeccionar los parámetros de direccionamiento del encabezado IP; el enrutador de salida de la red MPLS elimina de nuevo la etiqueta.

En efecto, MPLS crea «túneles» a través de una red IP enrutada para reenviar de forma eficiente paquetes que sigan una ruta fija y predecible. La conmutación de etiquetas evolucionó a partir de tecnologías punto a punto más antiguas orientadas a la conexión, tales como Frame Relay y el modo de transferencia asíncrona. MPLS conservó la eficiencia de reenvío que tenían las anteriores tecnologías de capa 2 (gracias a que llevaban el tráfico sobre una red IP enrutada de capa 3) y mejoró la flexibilidad de la red mediante la creación de «circuitos arrendados» virtuales que se pueden configurar sin necesidad de realizar en la red cambios físicos, de capa 2 o de la tabla de enrutamiento de capas.

Los «túneles» de conmutación de etiquetas permiten separar el tráfico de diferentes clientes en la red de un proveedor de servicios, lo que supone un método para formar redes VPN. También se utiliza para crear enrutamientos y reenvíos virtuales (VRF) dentro de la red privada de un único cliente. El contenido a continuación de la etiqueta MPLS del paquete IP puede cifrarse opcionalmente de manera integral, sin que ello obstaculice la capacidad de reenvío del paquete o su eficiencia, para ofrecer VPN o VRF seguros (o cifrados).

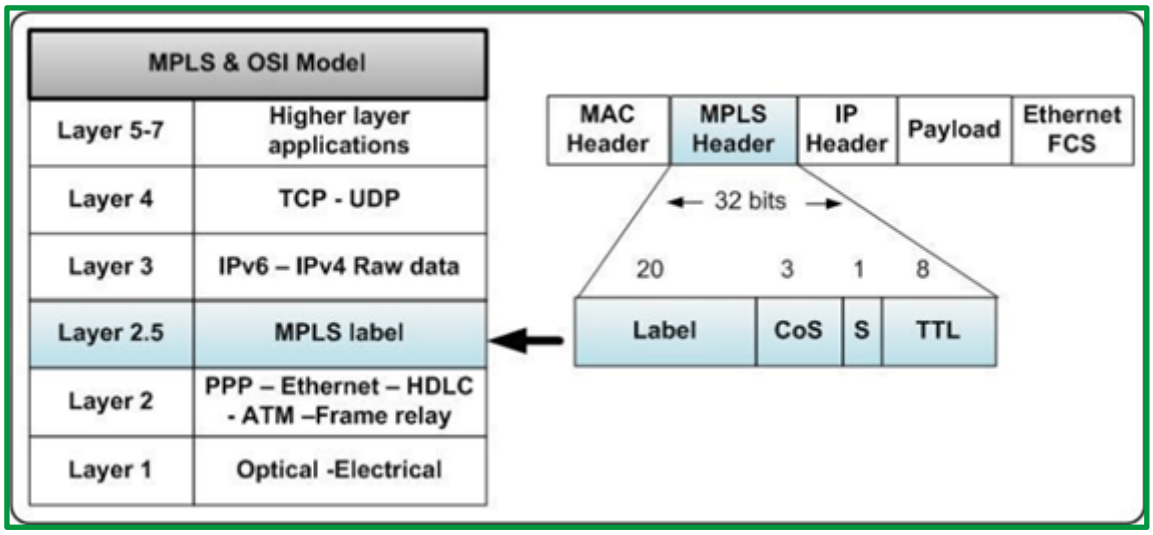


Figure 97:Tecnología MPLS

La cabecera MPLS contiene los siguientes campos:

- **Label** Value: valor de la etiqueta (20 bits)
- **EXP**: indicador de CoS, Class of Service (3 bits)
- **S**: BoS (Bottom of Stack, 1 bit), se utiliza para identificar la última etiqueta.
- **TTL**: Time To Live, indica por cuántos nodos puede pasar un paquete antes de ser descartado (8 bits)

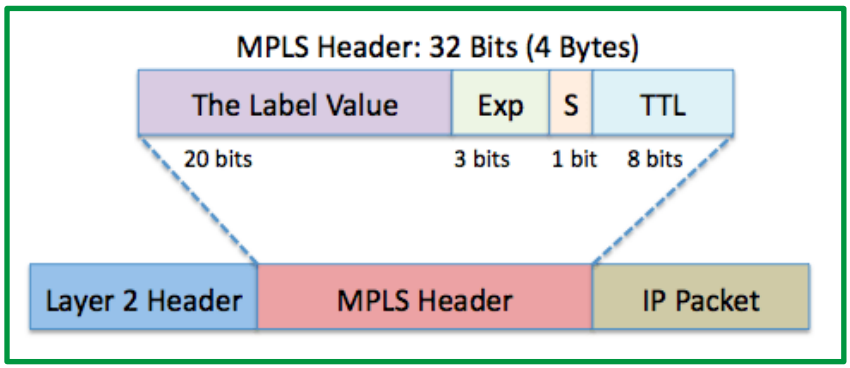


Figure 98: Cabecera MPLS

Point-to-Point Protocol (PPP)

El Protocolo punto a punto (PPP) ofrece un método estándar para transportar datagramas multiprotocolo a través de enlaces de punto a punto. PPP está conformado por tres componentes principales:

- Entramado del estilo de **HDLC**, método para encapsular datagramas multiprotocolo.
- Un protocolo de control de enlace (**LCP**) para establecer, configurar y probar la conexión de enlace de datos.
- Una familia de protocolos de control de red (**NCP**) para establecer y configurar distintos protocolos de capa de red.

PPP encapsula tramas de datos para transmitirlas a través de enlaces físicos de capa 2. PPP establece una conexión directa mediante cables seriales, líneas telefónicas, líneas troncales, teléfonos celulares, enlaces de radio especializados o enlaces de fibra óptica.

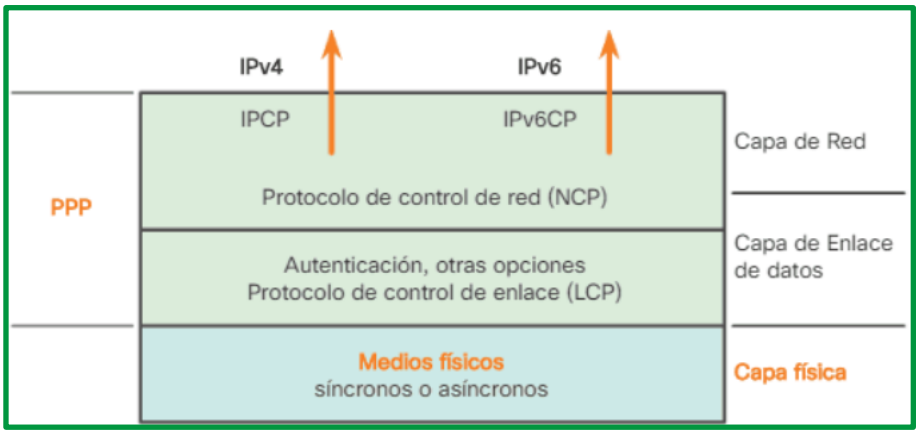


Figure 99: Distribución de las funciones LCP y NCP protocolo PPP

En la capa física, puede configurar PPP en un rango de interfaces, incluidas las siguientes:

- Serial asíncrono
- Serial síncrono
- HSSI
- ISDN

PPP opera a través de cualquier interfaz DTE/DCE (RS-232-C, RS-422, RS-423 o V.35). El único requisito absoluto impuesto por PPP es un circuito full-duplex, ya sea dedicado o conmutado, que pueda funcionar en modo de bits seriales síncrono o asíncrono, transparente para las tramas de capa de enlace PPP.

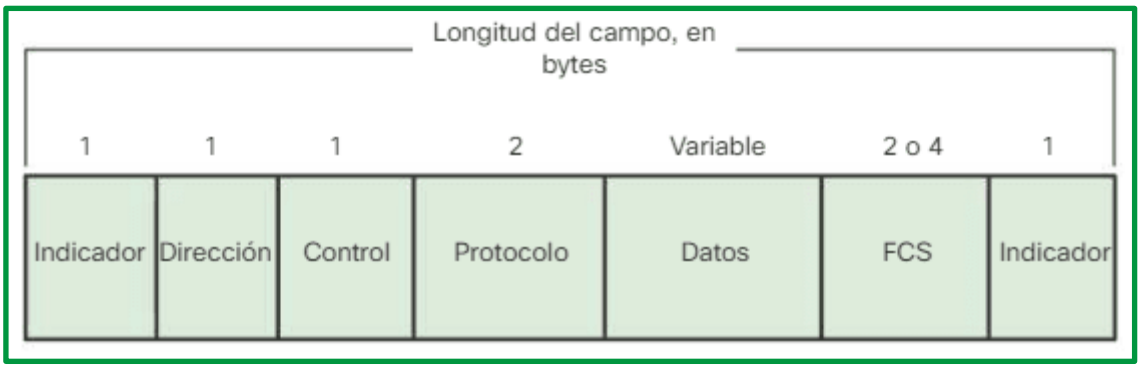


Figure 100: Trama PPP

La trama PPP está compuesta por los siguientes elementos:

- **Indicador**: un único byte que indica el inicio y el final de una trama. El campo Señalización está formado por la secuencia binaria 01111110. En tramas PPP sucesivas sólo se usa un caracter de señalador único.

- **Dirección**: un único byte que contiene la secuencia binaria 11111111, la dirección de difusión estándar. PPP no asigna direcciones a estaciones individuales.
- **Control**: un único byte formado por la secuencia binaria 00000011, que requiere la transmisión de datos de usuario en una trama no secuencial.
- **Protocolo**: dos bytes que identifican el protocolo encapsulado en el campo de información de la trama. El campo Protocolo de 2 bytes identifica al protocolo del contenido PPP.
- **Datos**: cero o más bytes que contienen el datagrama para el protocolo especificado en el campo Protocolo. Para encontrar el fin del campo de información, se debe buscar la secuencia del indicador de finalización y dejar 2 bytes para el campo FCS.
- **Secuencia de verificación de trama (FCS)**: normalmente de 16 bits (2 bytes). Mediante un acuerdo previo, con la aceptación de las implementaciones PPP se puede utilizar una FCS de 32 bits (4 bytes) para una mayor detección de errores.

Encapsulación WAN

Los datos de la capa de red se envían a la capa de enlace de datos para ser transmitidos a través de un enlace físico que normalmente es de punto a punto sobre una conexión WAN. La capa de enlace de datos crea una trama alrededor de los datos de la capa de red, de modo que se apliquen los controles y verificaciones necesarias. Cada tipo de conexión WAN utiliza un protocolo de Capa 2 para encapsular un paquete mientras atraviesa el enlace WAN. Para asegurarse de que se esté utilizando el protocolo de encapsulación correcto, se debe configurar el tipo de encapsulación de Capa 2 utilizado en cada interfaz serial del router. El protocolo de encapsulación que se debe usar depende de la tecnología WAN y del equipo. HDLC fue propuesto en 1979 y, por este motivo, la mayoría de los protocolos de entramado que se desarrollaron después se basan en él.

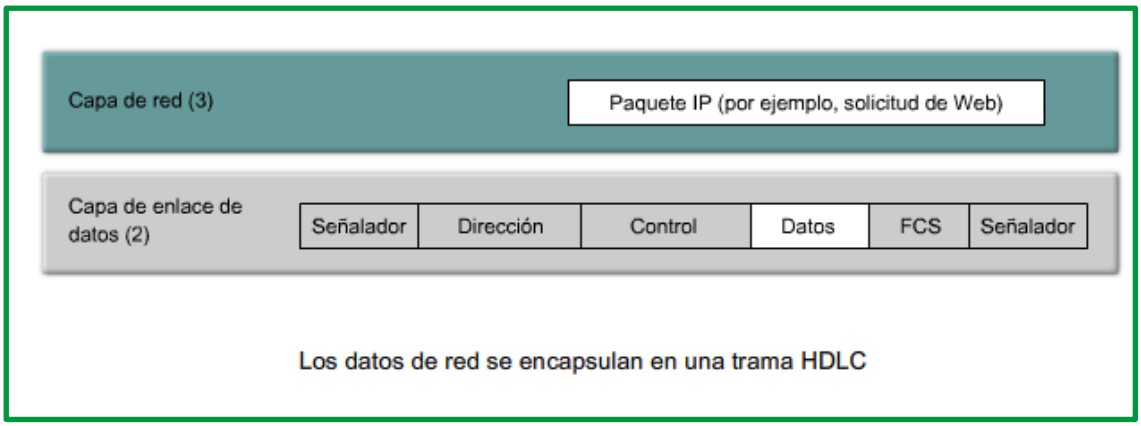


Figure 101: Encapsulación de trama HDLC

Formatos de encapsulación de tramas WAN

Al examinar la porción del encabezado de una trama HDLC, se pueden identificar campos comunes que utilizan muchos protocolos de encapsulación WAN. La trama siempre comienza y termina con un campo de señaladores de 8 bits. El patrón de los bits es 01111110. El campo de la dirección no se necesita para enlaces WAN, que casi siempre son

punto a punto. Aun así, el campo de la dirección está presente y puede ocupar 1 o 2 bits. El campo de control depende del protocolo, pero normalmente indica si el contenido de los datos es información de control o si se trata de datos de la capa de red. El campo de control normalmente ocupa 1 byte.

Juntos, los campos de control y la dirección se denominan encabezado de la trama. El dato encapsulado sigue el campo de control. Entonces, una secuencia de verificación de trama (FCS, frame check sequence) utiliza el mecanismo de comprobación de redundancia cíclica (CRC, cyclic redundancy check) para establecer un campo de 2 o 4 bytes.

Se utilizan varios protocolos de enlace de datos, incluidos subgrupos y versiones propietarias de HDLC. Tanto PPP como la versión de Cisco de HDLC tienen un campo adicional en el encabezado para identificar el protocolo de capa de red de los datos encapsulados.

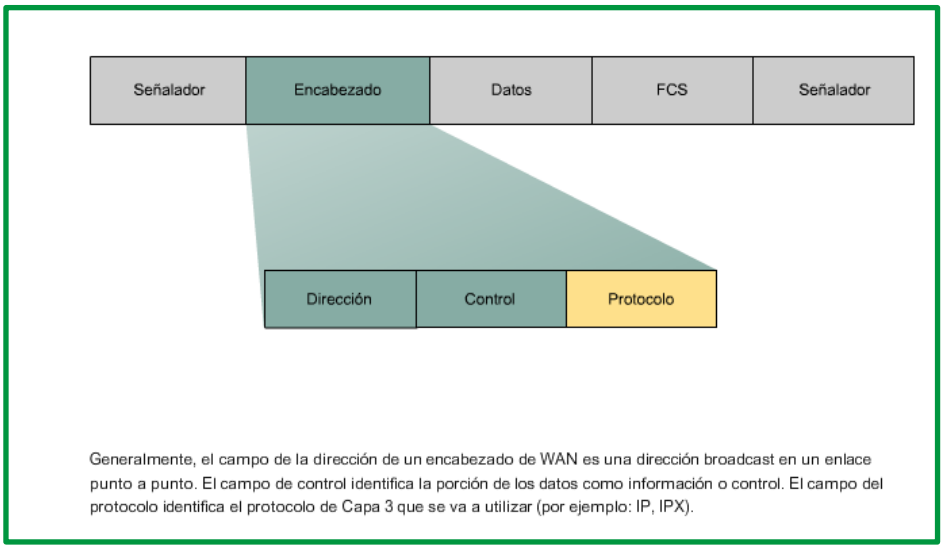


Figure 102: Encabezado de encapsulación dé trama WAN

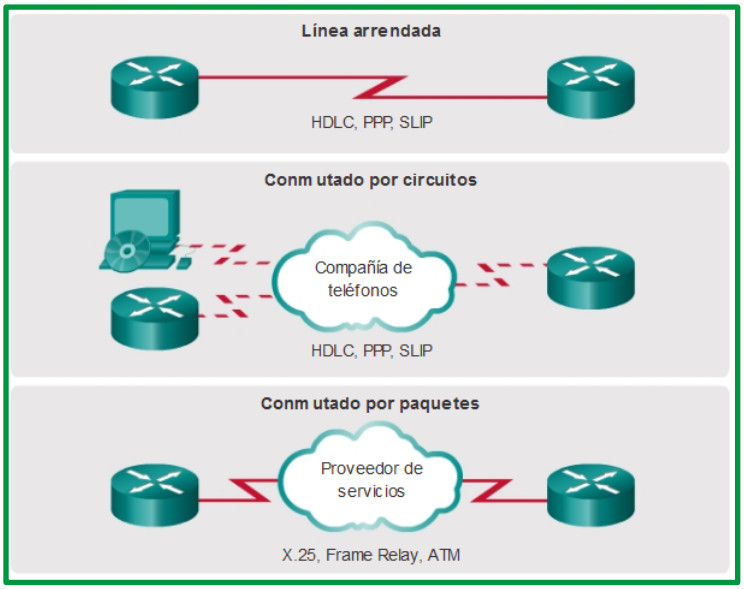


Figure 103: Protocolos de encapsulación WAN

Subcapa de Control de Acceso al medio

El control de acceso al medio en informática y telecomunicaciones, es el conjunto de mecanismos y protocolos por los que varios "interlocutores" (dispositivos en una red, como ordenadores, teléfonos móviles, etc.) se ponen de acuerdo para compartir un medio de transmisión común (por lo general, un cable eléctrico u óptico, o en comunicaciones inalámbricas el rango de frecuencias asignado a su sistema)

La capa de enlace de datos se divide en dos subcapas:

- **Control de enlace lógico (LLC):** se trata de la subcapa superior, que define los procesos de software que proporcionan servicios a los protocolos de capa de red. El LLC coloca en la trama información que identifica qué protocolo de capa de red se utiliza para la trama. Esta información permite que varios protocolos de la capa 3, tales como IPv4 e IPv6, utilicen la misma interfaz y los mismos medios de red.
- **Control de acceso al medio (MAC):** se trata de la subcapa inferior, que define los procesos de acceso al medio que realiza el hardware. Proporciona el direccionamiento de la capa de enlace de datos y la delimitación de los datos de acuerdo con los requisitos de señalización física del medio y con el tipo de protocolo de capa de enlace de datos en uso.

La separación de la capa de enlace de datos en subcapas permite que un tipo de trama definido por la capa superior acceda a distintos tipos de medios definidos por la capa inferior. Tal es el caso en muchas tecnologías LAN, incluida Ethernet.

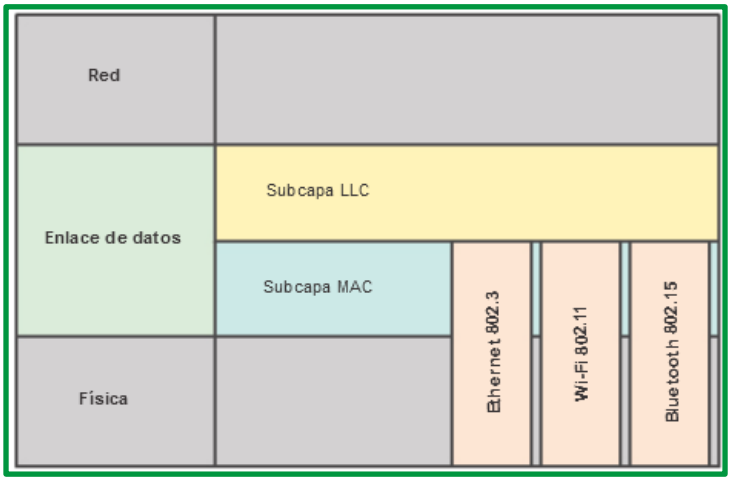


Figure 104:Subcapa de enlace de datos

En la figura, se muestra la forma en que la capa de enlace de datos se divide en las subcapas LLC y MAC. El LLC se comunica con la capa de red, mientras que la subcapa MAC admite diversas tecnologías de acceso de red. Por ejemplo, la subcapa MAC se comunica con la tecnología LAN Ethernet para enviar y recibir las tramas a través de cables de cobre o de

fibra óptica. La subcapa MAC también se comunica con tecnologías inalámbricas como Wi-Fi y Bluetooth para enviar y recibir tramas en forma inalámbrica.

Algunas de las funciones de la subcapa MAC incluyen:

- Controlar el acceso al medio físico de transmisión por parte de los dispositivos que comparten el mismo canal de comunicación.
- Agregar la dirección MAC del nodo fuente y del nodo destino en cada una de las tramas que se transmiten.
- Al transmitir en origen debe delimitar las tramas agregando bits de bandera (flags) para que el receptor pueda reconocer el inicio y fin de cada trama.
- Al recibir en destino debe determinar el inicio y el final de una trama de datos dentro de una cadena de bits recibidos por la capa física.
- Efectuar detección y, si procede, corrección de errores de transmisión.
- Descartar tramas duplicadas o erróneas.

En las redes de computadoras, la dirección MAC (siglas en inglés de media access control; en español "control de acceso al medio") es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo. Está determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits) utilizando el organizationally unique identifier. La mayoría de los protocolos que trabajan en la capa 2 del modelo OSI usan una de las tres numeraciones manejadas por el IEEE: MAC-48, EUI-48, y EUI-64, las cuales han sido diseñadas para ser identificadores globalmente únicos. No todos los protocolos de comunicación usan direcciones MAC, y no todos los protocolos requieren identificadores globalmente únicos.

Las direcciones MAC son únicas a nivel mundial, puesto que son escritas directamente, en forma binaria, en el hardware en su momento de fabricación. La dirección MAC es utilizada en varias tecnologías entre las que se incluyen:

- Ethernet
- 802.3 CSMA/CD
- 802.5 o redes en anillo a 4 Mbps o 16 Mbps
- 802.11 redes inalámbricas (Wi-Fi).

MAC opera en la capa 2 del modelo OSI, encargada de hacer fluir la información libre de errores entre dos máquinas conectadas directamente. Para ello se generan tramas, pequeños bloques de información que contienen en su cabecera las direcciones MAC correspondiente al emisor y receptor de la información.

Métodos de Acceso al Medio

En un entorno de medios compartidos, todos los dispositivos tienen acceso garantizado al medio, pero no tienen ninguna prioridad en dicho medio. Si más de un dispositivo realiza una transmisión simultáneamente, las señales físicas colisionan y la red debe recuperarse

para que pueda continuar la comunicación. Las colisiones representan el precio que debe pagar la Ethernet para obtener la sobrecarga baja que se relaciona con cada transmisión. Ethernet utiliza el acceso múltiple por detección de portadora y detección de colisiones (CSMA/CD) para detectar y manejar colisiones.

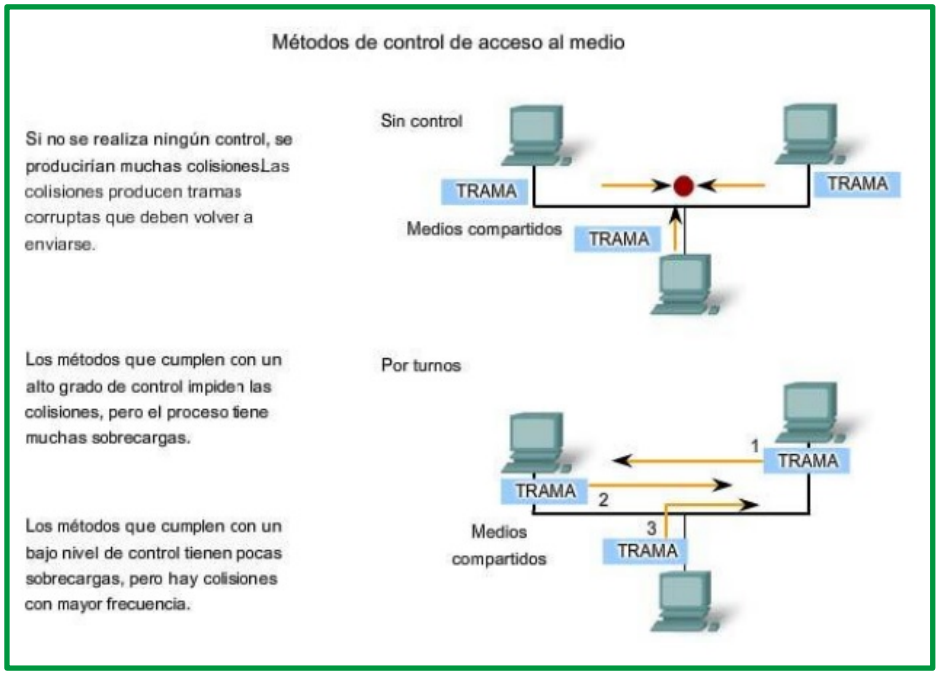


Figure 105: Métodos de control de acceso al medio

CSMA/CD

CSMA/CD son siglas que corresponden a las siglas Carrier Sense Multiple Access with Collision Detection, que corresponden a Acceso Múltiple por Detección de Portadora con Detección de Colisiones, es una técnica usada en las redes para mejorar las prestaciones. La meta de este protocolo es de evitar al máximo las colisiones.

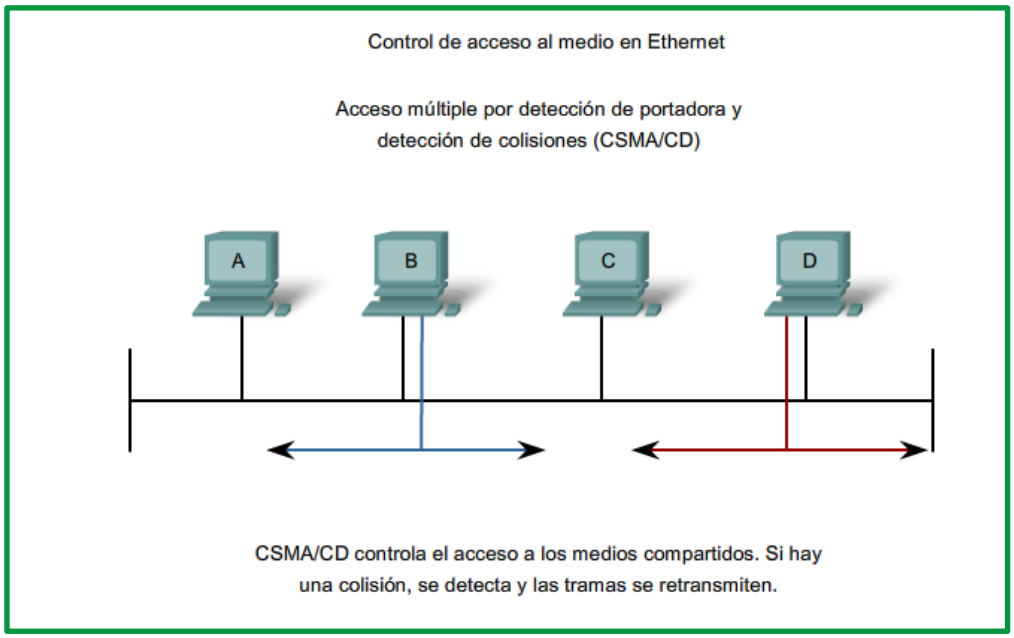


Figure 106. CSMA/CD

El funcionamiento de CSMA/CD se establece de la siguiente forma:

1. Una estación que tiene un mensaje para enviar escucha al medio para ver si otra estación está transmitiendo un mensaje.
2. Si el medio está libre (ninguna otra estación está transmitiendo), se envía la transmisión y se espera el ACK (acuse de recibo). La estación que recibe comprueba el CRC (detección de errores) y si es correcto envía el ACK. Si tras un tiempo no ha sido recibido el ACK, se pasa al paso 1. Si se recibe, la operación ha sido un éxito.
3. Cuando dos o más estaciones tienen mensajes para enviar, es posible que transmitan casi en el mismo instante, resultando en una colisión en la red.
4. Cuando se produce una colisión, todas las estaciones receptoras ignoran la transmisión confusa.
5. Si un dispositivo de transmisión detecta una colisión, envía una señal de expansión para notificar a todos los dispositivos conectados que ha ocurrido una colisión.
6. Las estaciones transmisoras detienen sus transmisiones tan pronto como detectan la colisión.
7. Cada una de las estaciones transmisoras espera un periodo de tiempo aleatorio e intenta transmitir otra vez.

Detección de portadora

En el método de acceso CSMA/CD, todos los dispositivos de red que tienen mensajes para enviar deben escuchar antes de transmitir. Si un dispositivo detecta una señal de otro dispositivo, esperará durante un período especificado antes de intentar transmitir. Cuando no se detecte tráfico, un dispositivo transmitirá su mensaje. Mientras se lleva a cabo la transmisión, el dispositivo continúa escuchando para detectar tráfico o colisiones en la LAN.

Una vez que se envía el mensaje, el dispositivo regresa a su modo de escucha predeterminado.

Acceso múltiple

Puede darse el caso de que un segundo dispositivo no detecte las señales y comience también a transmitir. Los medios tienen entonces dos dispositivos que transmiten sus señales al mismo tiempo. Sus mensajes se propagarán por todos los medios hasta que se encuentren. En ese punto, las señales se mezclan y el mensaje se destruye.

Detección de colisiones

Cuando un dispositivo está en el modo de escucha, puede detectar cuando se produce una colisión en el medio compartido. La detección de una colisión es posible porque todos los dispositivos pueden detectar un aumento de la amplitud de la señal por encima del nivel normal. Una vez que se produce una colisión, los demás dispositivos que están en el modo de escucha, así como todos los dispositivos de transmisión, detectan el aumento de amplitud de la señal. Una vez detectada la colisión, todos los dispositivos transmisores continuarán transmitiendo para garantizar que todos los dispositivos de la red detecten la colisión.

Señal de congestión y postergación aleatoria

Cuando los dispositivos de transmisión detectan la colisión, envían una señal de congestión. Esta señal de congestión se utiliza para notificar a los demás dispositivos sobre una colisión, de manera que éstos invocarán un algoritmo de postergación. Este algoritmo de postergación hace que todos los dispositivos dejen de transmitir durante un período aleatorio, lo que permite que las señales de colisión disminuyan. Una vez que finaliza el retraso asignado a un dispositivo, dicho dispositivo regresa al modo "escuchar antes de transmitir". El período de postergación aleatoria garantiza que los dispositivos involucrados en la colisión no intenten enviar su tráfico nuevamente al mismo tiempo, lo que provocaría que se repita todo el proceso.

Tipos de CSMA/CD

En función de cómo actúe la estación, el método CSMA/CD se puede clasificar en:

- **CSMA no-persistente**: si el canal está ocupado espera un tiempo aleatorio y vuelve a escuchar. Si detecta el canal libre, emite.
- **CSMA 1-persistente**: con el canal ocupado, la estación pasa a escuchar constantemente el canal sin esperar ningún tiempo. Cuando lo detecta libre emite. Podría ocurrir que emitiera otra estación durante un retardo de propagación o latencia de la red posterior a la emisión de la trama, produciéndose una colisión.
- **CSMA p-persistente**: después de encontrar el canal ocupado y quedarse escuchando hasta encontrarlo libre, la estación decide si emite. Para ello ejecuta un algoritmo o

programa que dará orden de transmitir con una probabilidad p, o de permanecer a la espera. Si no transmitiera, en la siguiente ranura o división de tiempo volvería a ejecutar el mismo algoritmo hasta transmitir. Así se reduce el número de colisiones.

Paso de testigo

Es un método determinístico ya que se garantiza el acceso de cualquier estación a la red en un tiempo máximo. Esta técnica de control distribuido se basa en una trama especial o testigo que va pasando por todas las estaciones de la red.

Cuando una estación quiere transmitir datos coge el testigo y lo transforma en una trama de información, esta trama circula por toda la red hasta que llega a la estación destino que recogerá la información y enviará de vuelta el testigo a la estación origen, así comprobará que han llegado los datos a su destino y pasará el testigo a la siguiente estación. Este método se puede utilizar con topologías en anillo, en bus y en estrella y con distintos tipos de redes como son: Token Bus, Token Ring, FDDI. Con esta técnica no se puede dar una colisión por lo que es mejor para situaciones de mucho tráfico y para obtener un rendimiento homogéneo de todas las estaciones.

Un ejemplo de este tipo de redes son las Token Ring que tiene su topología lógica en forma de anillo.

Funcionamiento:

Su principio básico de funcionamiento en esta red se basa en que si un nodo de la red tiene datos para enviar debe tomar un token libre, la cual se realiza modificando un bit en el segundo byte del token. En el caso de que no tenga datos para enviar deberá pasar el token a la siguiente estación de la red.

Los nodos pueden apropiarse del token por un tiempo máximo y durante este tiempo las otras estaciones permanecen inactivas.

Al terminar la Trasmisión el token queda libre y de ahí puede ser utilizado por alguna otra estación de la Red, esto se realiza para poder evitar colisiones.

Ventajas:

- Existe igualdad entre todos los nodos que conforman la red.
- Es una red que en su mayoría evita colisiones.

Desventajas:

- Es una red en la cual es muy difícil ingresar otra estación y al implementarla debería estar fuera de servicio.
- Tiene limitación de Velocidad.

Lectura complementaria de la asignatura

En el sitio web de la empresa **DarFe** se encuentran el libro de ***seguridad por niveles*** de autoría de Alejandro Corletti Estrada que se sugiere realizar lectura. Sitio web : https://www.darfe.es . Estará publicado en plataforma como recursos complementarios

.

Bibliografía

ccnadesdecero.es. (s.f.). *Aprende Redes con Cisco CCNA desde Cero*. Recuperado el 10 de 05 de 2021, de https://ccnadesdecero.es

EcuRed. (s.f.). *Conmutación* . Recuperado el 10 de 05 de 2021, de https://www.ecured.cu/

electronicafacil.net. (s.f.). *Electronica Facil*. Recuperado el 10 de 05 de 2021, de https://www.electronicafacil.net/tutoriales/

Instituto Tècnologico de Roque. (s.f.). *Cisco Networking Academy*. Recuperado el 10 de 05 de 2021, de http://itroque.edu.mx/cisco/cisco1/

Jiménez, E. S. (s.f.). *Universidad Oberta de Cataluña*. Recuperado el 10 de 05 de 2021, de http://openaccess.uoc.edu

MeetUp Tech Club Tajamar. (22 de 05 de 2019). Recuperado el 10 de 05 de 2021, de https://techclub.tajamar.es/red-mpls/

Netwgeeks. (05 de 03 de 2019). Recuperado el 10 de 05 de 2021, de https://netwgeeks.com/

Pontificia Universidad Católica del Perú. (s.f.). *Repositorio Institucional de la PUCP*. Recuperado el 10 de 05 de 2021, de http://repositorio.pucp.edu.pe

Roldán, J. T. (01 de 02 de 2006). *Colecciòn de Tesis Digitales de la Universidad de las Americas Puebla*. Recuperado el 10 de 05 de 2021, de http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/

Ruiz, F. R. (s.f.). *Universidad Oberta de Cataluña*. Recuperado el 10 de 05 de 2021, de http://openaccess.uoc.edu

Serra, X. H. (2002). *books.google.com*. Recuperado el 10 de 05 de 2021, de https://books.google.com.ec/books?id=11DSMYYKvL0C&lpg=PA5&dq=inauthor%3A%22Xavier%20Hesselbach%20Serra%22&hl=es&pg=PA5#v=onepage&q&f=false

sites.google.com. (s.f.). Recuperado el 10 de 05 de 2021, de https://sites.google.com/site/redeslocalesyglobales/

The TCP/IP Guiede. (05 de 09 de 2005). Recuperado el 10 de 05 de 2021, de http://www.tcpipguide.com/

Universida Tecnica Nacional. (s.f.). *Modulaciòn Digital*. Recuperado el 10 de 05 de 2021, de https://utn.edu.ar/es/

Universidad Autònoma de Hidalgo. (s.f.). *Centro de Innovación para el Desarrollo y la Capacitación en Materiales Educativos*. Recuperado el 10 de 05 de 2021, de http://cidecame.uaeh.edu.mx/

Universidad Catòlica Santiago de Guayaquil. (04 de 03 de 2020). *Repositorio Digital UCSG*. Recuperado el 10 de 05 de 2021, de http://repositorio.ucsg.edu.ec

Universidad de Cantabria. (2005). *Escuela Técnica Superior de Ingenieros Industriales y de Telecomunicación* . Recuperado el 10 de 05 de 2021, de https://www.ctr.unican.es/asignaturas/instrumentacion_5_IT/

Universidad de Oviedo. (05 de 03 de 2012). *Departamento de Ingeniería Eléctrica, Electrónica, de Computadores y de Sistemas*. Recuperado el 10 de 05 de 2021, de http://www.isa.uniovi.es/docencia/redes/

Universidad de Valladolid. (20116). *Instrumentación para las telecomunicaciones* . Recuperado el 10 de 05 de 2021, de https://www.ele.uva.es/index_electronica.html

Universidad de Vigo. (2003). *Dpto. Enxeñería Eléctrica / Dpt. of Electrical Engineering*. Recuperado el 10 de 05 de 2021, de http://grupo_ene.webs.uvigo.es/wordpress/publicaciones/Apuntes_Fourier.pdf

Universidad del Cauca. (2019). Recuperado el 10 de 05 de 2021, de http://dtm.unicauca.edu.co/pregrado/conmutacion/transp/

Universidad Nacional del Nordeste. (s.f.). *Departamento de Informática*. Recuperado el 10 de 05 de 2021, de http://exa.unne.edu.ar

Universidad Politecnica de Cartagena. (2010). *ETS Ingenieria de Telecomunicaciones*. Recuperado el 10 de 05 de 2021, de https://ocw.bib.upct.es/

El contenido y gráficos de este compendio han sido obtenido mayoritariamente del curso CCNA de la academia de CISCO, información complementada con información de sitios web que se establecen en las referencias bibliográfica.

Índice

Tabla de contenido

Organización de la lectura para el estudiante por semana del compendio

Semanas	Paginas
Semana 8	Página 3 - 44
Semana 9	Página 45 - 95
Semana 10	Página 96 – 117
Semana 11	Página 117 – 169
Semana 12	Página 177

Resultado de aprendizaje de la asignatura

Conocer los principios básicos, componentes, dispositivos, protocolos, estándares y demás elementos que intervienen en una red de comunicación.

REDES DE COMPUTADORAS

Unidad 3: **Capa de Red y Direccionamiento IPv4/IPv6**

Resultado de aprendizaje de la unidad:

Utilizar el direccionamiento de redes para dividir una red en varias subredes según las aplicaciones que va implementar.

Conocer los principios que deben considerarse a nivel de red, desde su correcto diseño y segmentación hasta el enrutamiento de los paquetes de datos aplicando criterios principales como métricas, tecnologías aplicadas, equipos utilizados, protocolos, entre otros.

La Capa de red o Capa 3 de OSI provee servicios para intercambiar secciones de datos individuales a través de la red entre dispositivos finales identificados. Para realizar este transporte de extremo a extremo la Capa 3 utiliza cuatro procesos básicos:

- Direccionamiento,
- Encapsulamiento,
- Enrutamiento, y
- Desencapsulamiento.

Algunas de las funciones del nivel de red son:

- Encaminamiento: elegir la ruta más adecuada para que el bloque de datos de este nivel paquete) llegue a su destino.
- Tratamiento de la congestión evitando cuellos de botella en la red.
- Resolución de problemas relacionados con redes heterogéneas: sistemas de direccionamiento distintos, paquetes de distintas dimensiones, etc.

La capa de red se ocupa de la obtención de paquetes procedentes de la fuente y enrutarle durante el camino hasta que pueda alcanzar su destino; Para llegar al destino pueden surgir la necesidad de hacer varios saltos en nodos intermedios.

Los nodos intermedios se denominan también IMP (procesadores de intercambio de mensaje), router o encaminadores.

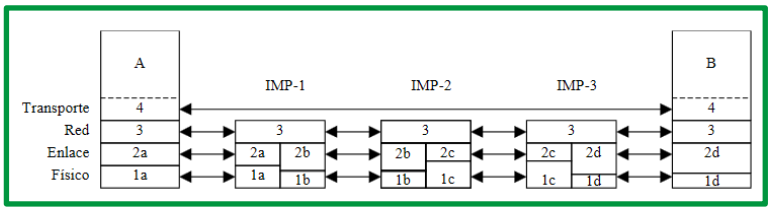


Figure 1. Nodos intermedios (IMP – Router - Encaminadores)

Para alcanzar el destino, la capa de red tiene que conocer la topología de las subredes de comunicación establecidas seleccionando la mejor ruta y solventando los problemas que se presente.

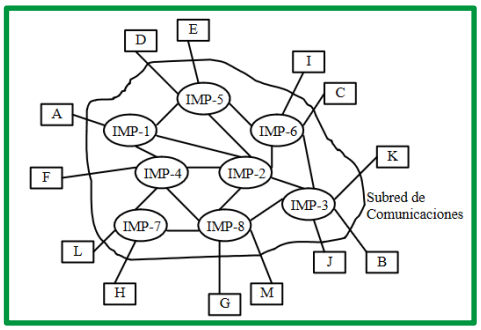


Figure 2. Subredes de comunicaciones

Un router es una computadora. El primer router, utilizado para la Red de la Agencia de Proyectos de Investigación Avanzada (ARPANET), fue el Procesador de mensajes de interfaz (IMP). El IMP era una minicomputadora Honeywell 316; esta computadora dio origen a la ARPANET el 30 de agosto de 1969.

Los routers tienen muchos de los mismos componentes de hardware y software que se encuentran en otras computadoras, entre ellos:

- CPU
- RAM
- ROM
- Sistema operativo

Los routers usan protocolos de rutas estáticas y de enrutamiento dinámico para aprender sobre redes remotas y construir sus tablas de enrutamiento.

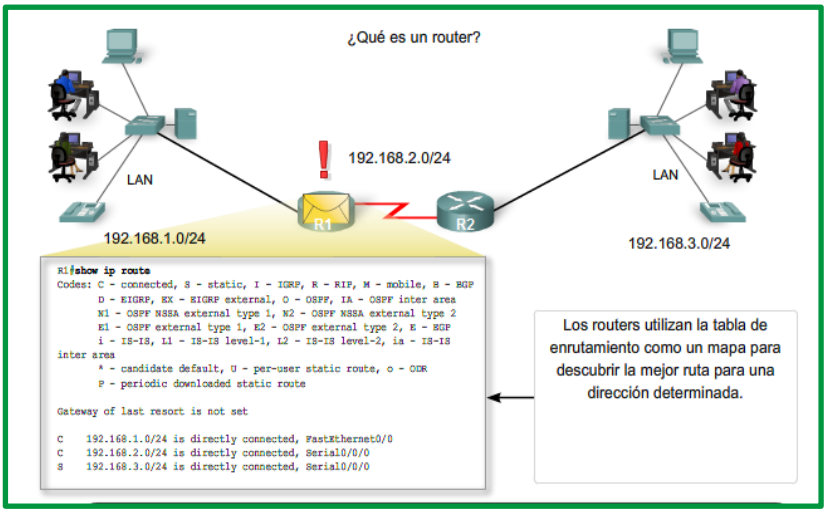


Figure 3. Datos de configuración de un router

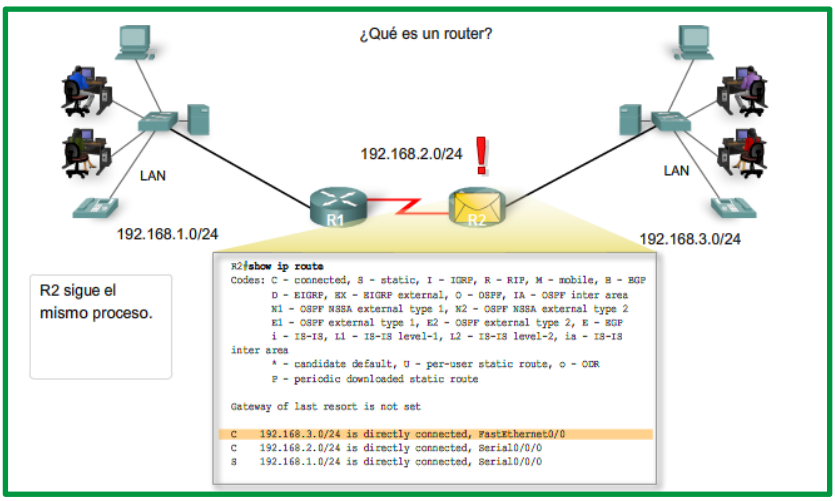


Figure 4. Datos de configuración de un router

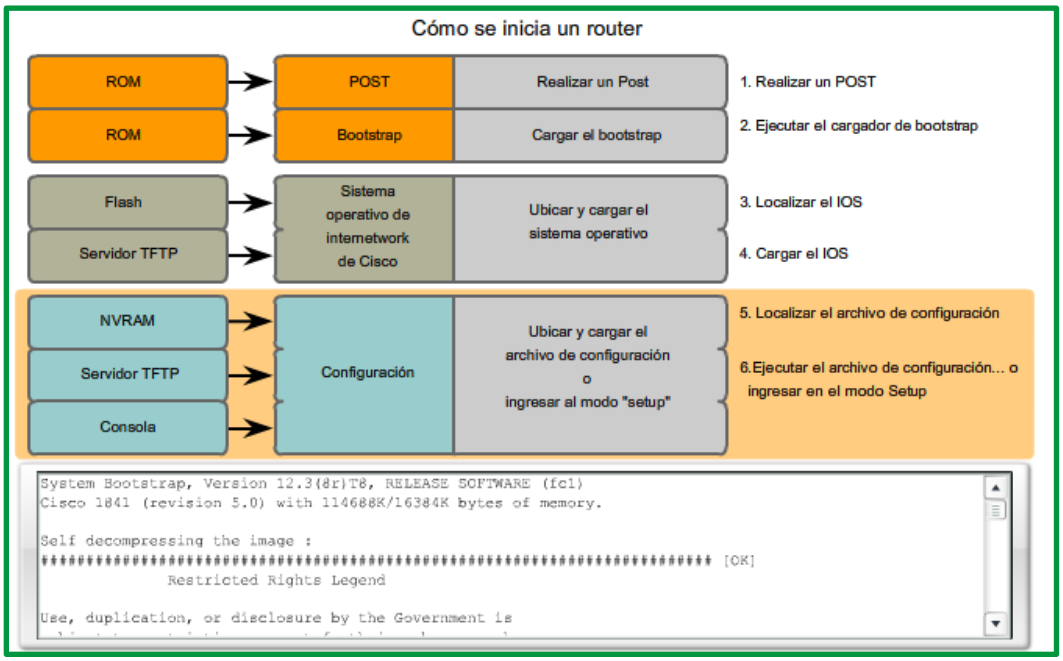


Figure 5. Proceso de arranque de un router

Las interfaces de los router pueden dividirse en dos grandes grupos principales:

- **Interfaces LAN**, como Ethernet y FastEthernet
- **Interfaces WAN**, como serial, ISDN y Frame Relay

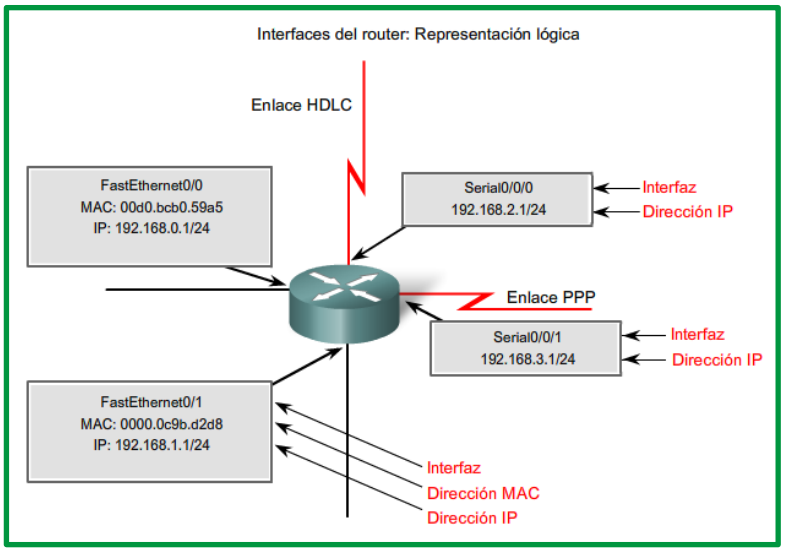


Figure 6. Representación lógica de las interfaces de un router

Routers y capa de Red

El objetivo principal de un router es conectar múltiples redes y enviar paquetes destinados ya sea a sus propias redes o a otras redes. Se considera al router como un dispositivo de Capa 3 porque su decisión principal de envío se basa en la información del paquete IP de Capa 3, específicamente la dirección IP de destino. Este proceso se conoce como enrutamiento.

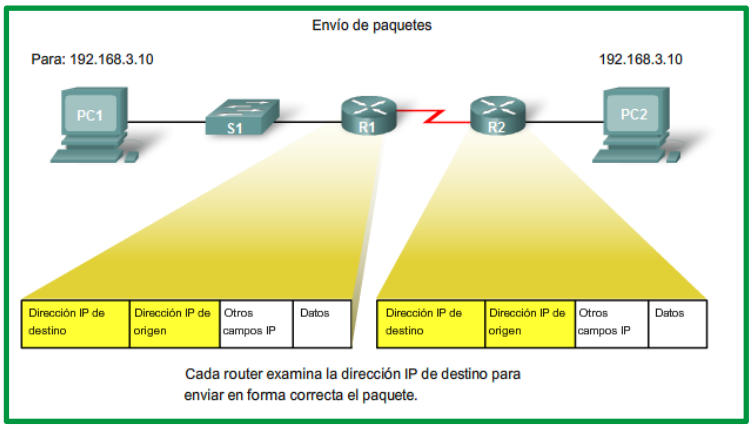


Figure 7. Proceso de enrutamiento que realiza un router

Cuando se diseña una nueva red o se hacen asignaciones en una red existente, es necesario documentar la red. Como mínimo, la documentación debe incluir un diagrama de topología que indique la conectividad física y una tabla de direccionamiento que mencione la siguiente información:

- Nombres de dispositivos,
- Interfaces usadas en el diseño,
- Direcciones IP y máscaras de subred, y
- Direcciones de gateway por defecto para dispositivos finales, como las PC.

Aspecto de diseño de la capa de red

La capa de red es la capa más baja que establece la transmisión de extremo a extremo mismo que conlleva a diversos aspectos sean considerados en el diseño de la red, entre estas tenemos:

- **Implementación del servicio orientada a la conexión**

  Considera los recursos que permiten establecer la conexión inicial de extremo a extremo y una vez finalizada la conexión deben cerrarse y liberarse los recursos. Al aplicar el servicio orientado a la conexión, antes de enviar cualquier paquete de datos es necesario establecer una ruta del enrutador de origen a destino; a esta conexión se la conoce como circuito virtual (CV), en analogía con los circuitos físicos establecido por el sistema telefónico.

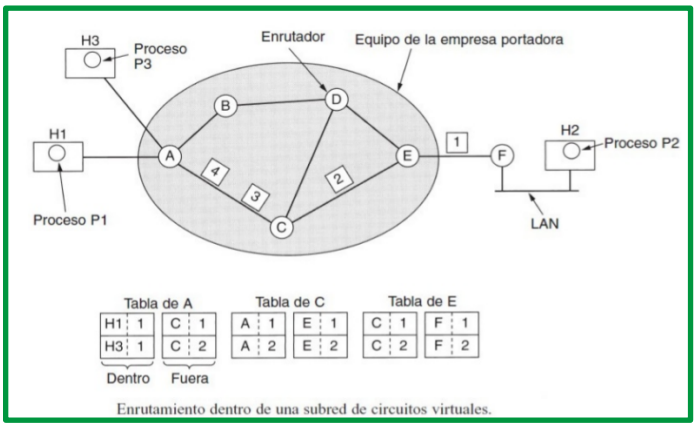


Figure 8. Enrutamiento dentro de una subred de CV.

- **Implementación del servicio no orientada a la conexión**

  Si se ofrece el servicio no orientado a la conexión, los paquetes se colocan de manera individual en la subred y se enrutan de manera independiente; en este contexto, los paquetes se conocen como datagramas.

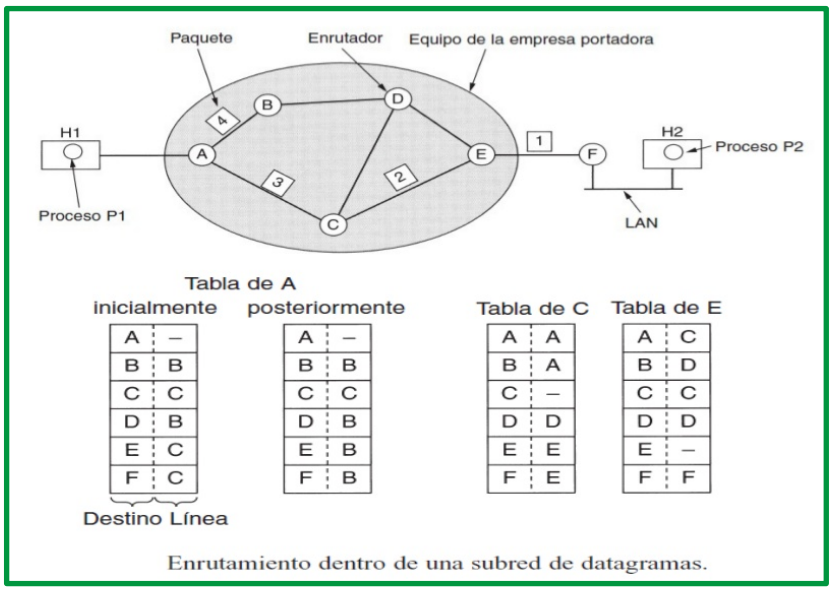


Figure 9. Enrutamiento dentro una subred de datagramas.

- **Conmutación de paquetes de almacenamiento y reenvió**

  En las redes de conmutación de paquete cada nodo intermedio recibe el mensaje en forma de paquetes de datos y los almacena hasta que los reenvía hacia su destino final a otro nodo intermedio.

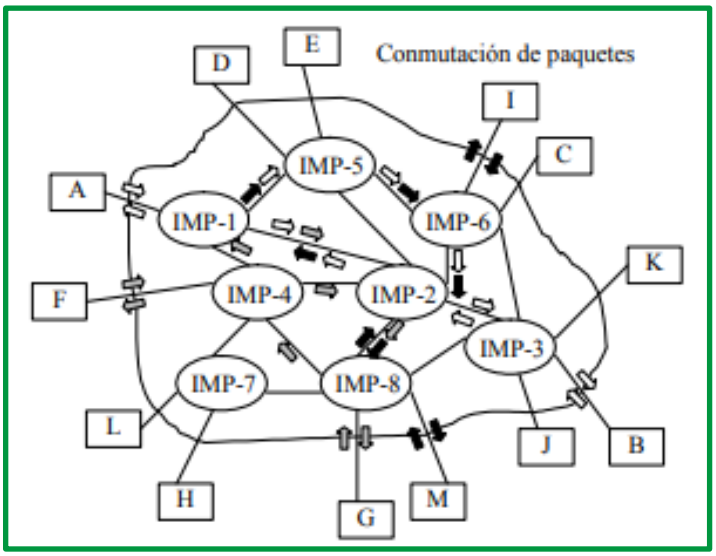


Figure 10. Conmutación de paquete

Las ventajas de la conmutación de paquetes frente a la de circuitos son:

1. La eficiencia de la línea es mayor: Ya que cada enlace se comparte entre varios paquetes que estarán en cola para ser enviados en cuanto sea posible. En conmutación de circuitos, la línea se utiliza exclusivamente para una conexión, aunque no haya datos a enviar.

2. Se permiten conexiones entre estaciones de velocidades diferentes: Esto es posible ya que los paquetes se almacenarán en cada nodo conforme lleguen en una cola y se irán enviando a su destino.

3. No se bloquean llamadas: Como todas las conexiones se aceptan, aunque si hay muchas, se producen retardos en la transmisión.

4. Se pueden usar prioridades: Un nodo puede seleccionar de su cola de paquetes en espera de ser transmitidos, aquellos más prioritarios según ciertos criterios de prioridad. Cuando un emisor necesita enviar un grupo de datos mayor que el tamaño fijado para un paquete, éste los divide en paquetes y los envía uno a uno al receptor. Hay dos técnicas básicas para el envío de estos paquetes:

Técnica de datagramas: Cada paquete se trata de forma independiente, es decir, el emisor enumera cada paquete, le añade información de control por ejemplo número de paquete, nombre, dirección de destino y lo envía hacia su destino. Puede ocurrir que, por haber tomado caminos diferentes, un paquete con número por ejemplo 6 llegue a su destino antes que el número 5. También puede ocurrir que se pierda el paquete número 4. Todo esto no lo sabe ni puede controlar el emisor, por lo que tiene que ser el receptor el encargado de ordenar los paquetes y saber los que se han perdido.

Técnica de circuitos virtuales: Antes de enviar los paquetes de datos, el emisor envía un paquete de control que es de Petición de Llamada, este paquete se encarga de establecer un camino lógico de nodo en nodo por donde irán uno a

uno todos los paquetes de datos. De esta forma se establece un camino virtual para todo el grupo de paquetes. Este camino virtual será numerado o nombrado inicialmente en el emisor y ser á el paquete inicial de Petición de Llamada el encargado de ir informando a cada uno de los nodos por los que pase de que más adelante irán llegando los paquetes de datos con ese nombre o número. De esta forma, el encaminamiento sólo se hace una vez. El sistema es similar a la conmutación de circuitos, pero se permite a cada nodo mantener multitud de circuitos virtuales a la vez.

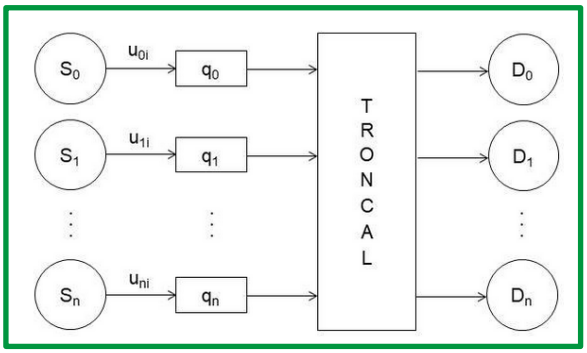


Figure 11. Red conmutada de paquetes con almacenamiento y reenvío
Autor: Eduardo Vargas

- **Servicios proporcionados a la capa de transporte**
  Se consideran los aspectos referentes a los servicios de red orientado a la conexión y servicios de red sin conexión.

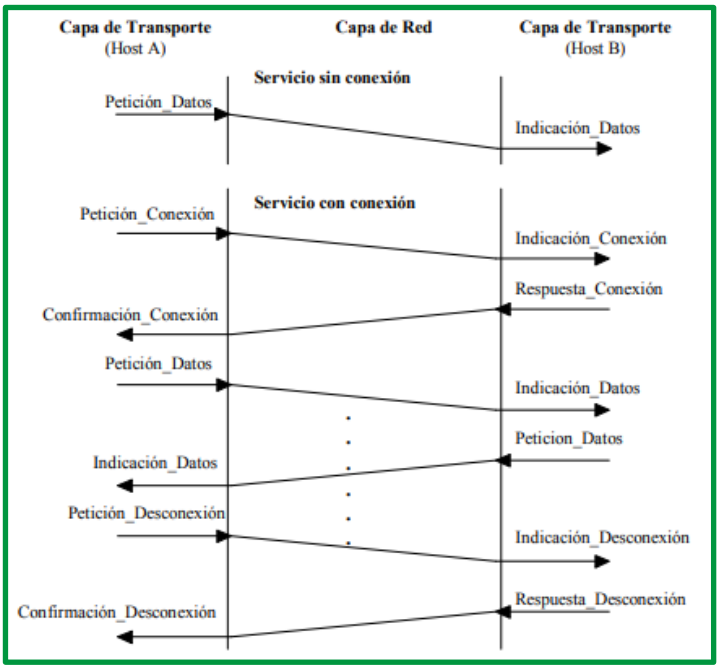


Figure 12. Ejemplo de la utilización de las primitivas básicas sin conexión y orientadas a la conexión de la capa de red

La primitivas tienen parámetros, por ejemplo, para establecer una conexión se usa la ***Petición_Conexión*** donde se especifica la dirección de red a la que se quiere conectar y la dirección de red que hace la llamada; también contiene otros parámetros que se utilizan

para solicitar servicios adicionales que son negociados entre las dos partes (Calidad del servicio donde se considera retardo, tasas de error, costo, entre otros).

En cuanto a las posibles combinaciones entre los servicios por la capa de la red y de enlace, las siguientes graficas representa ejemplos de cada una de ellas:

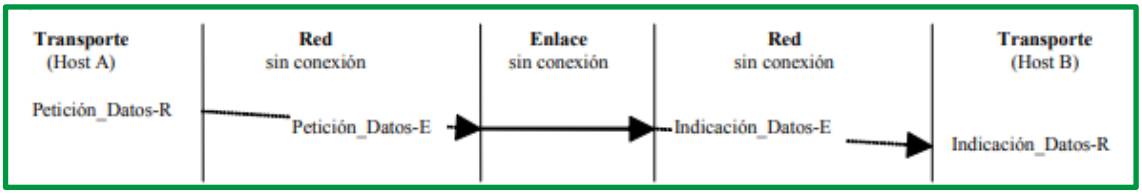


Figure 13. Capara de red sin servicio de conexión sobre una capa de enlace sin servicio de conexión

Convierte peticiones de envíos de paquetes de datos proveniente de la capa de transporte en peticiones de envió de una o varias tramas a través de la línea de enlace, ningunas de la capa asegura que lleguen los datos al destino ni que existan duplicidad de los mismo o que lleguen en el orden correcto los paquetes en la capa de red o de las tramas en la capa de enlace.

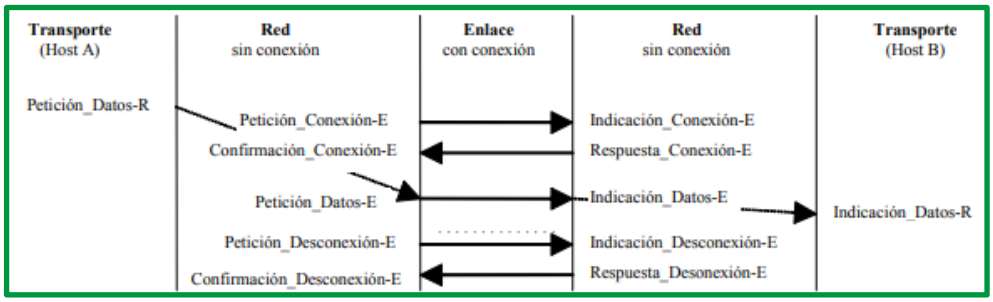


Figure 14. Capa de red sin servicio de conexión trabajando sobre una capa de enlace con servicio de conexión

Las tramas llegaran con seguridad, sin duplicidad y de forma ordenada; sin embrago la capa de red no asegura esto a la capa de transporte. Los paquetes de datos pueden perderse, duplicarse o cambiar el orden en el camino en los diferentes saltos entre IMP.

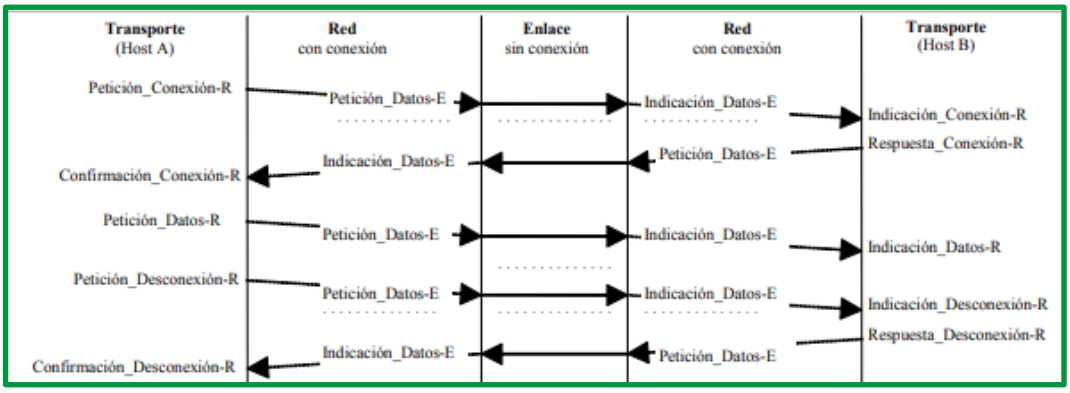


Figure 15. Capa de red con servicio de conexión trabajando sobre una capa de enlace sin servicio de conexión

Tiene como objetivo asegurar una conexión fiable a la capa de transporte a pesar de que la capa de enlace no sea fiable. Se deberá implementar mecanismos que permitan almacenar paquetes para su posible retransmisión, asegurar la correcta recepción de los mismos en los nodos de la red descartando posibles duplicados y manteniendo una correcta secuencia de los paquetes.

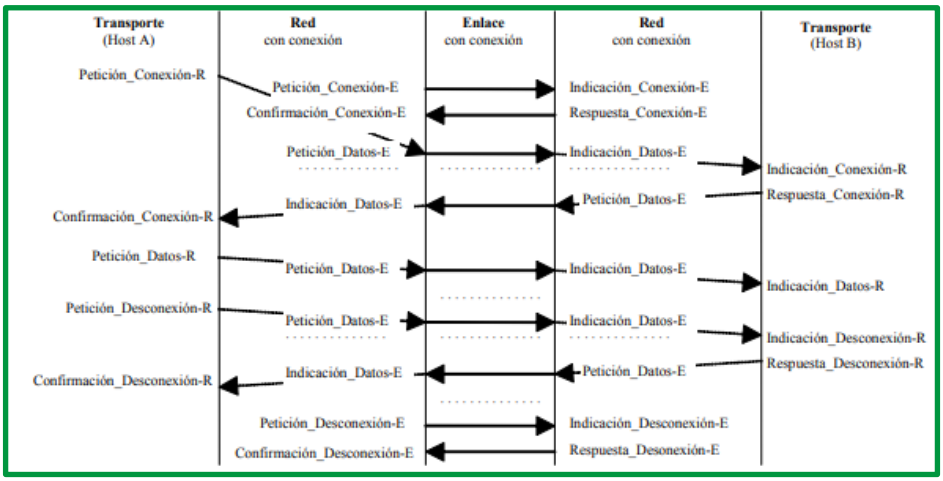


Figure 16. Capa de red con servicio de conexión trabajando sobre una capa de enlace con servicio de conexión

Se suele considerar que en las dos capas se implementan funciones redundantes para mantener la fiabilidad de las conexiones.

Otros aspectos que se deben considerar en los servicios proporcionados a la capa de transporte son:

- Los servicios deben ser independiente de la tecnología del enrutador.
- La capa de transporte debe estar aislada de la cantidad, tipo y tipología de los enrutadores presentes.
- Las direcciones de red disponibles para la capa de transporte deben seguir un plan de numeración uniforme, aun a través de varias LANs y WANs.

- **Comparación entre las subredes de circuitos virtuales y la de datagrama**

Se deben considerar que los circuitos virtuales y los datagramas tienen sus ventajas y desventajas.

Circuitos virtuales

Los circuitos virtuales utilizan números de circuitos en lugar de direcciones completas para identificar el origen y destino de la comunicación.

Los circuitos virtuales tienen problema de vulnerabilidad, si falla un IMP todos los circuitos virtuales establecidos en el tienen que ser abortados

- El concepto de circuito virtual se refiere a una asociación bidireccional, a través de la red, entre dos ETD, circuito sobre el cual se realiza la transmisión de los paquetes.

- Al inicio, se requiere una fase de establecimiento de la conexión, denominado: "llamada virtual"
- Durante la llamada virtual los ETDs se preparan para el intercambio de paquetes y la red reserva los recursos necesarios para el circuito virtual.
- Los paquetes de datos contienen sólo el número del circuito virtual para identificar al destino.
- Si la red usa encaminamiento adaptativo, el concepto de circuito virtual garantiza la secuenciación de los paquetes, a través de un protocolo fin-a-fin (nodo origen/nodo destino).
- El concepto de CV permite a un ETD establecer caminos de comunicación concurrentes con varios otros ETDs, sobre un único canal físico de acceso a la red.
- El CV utiliza al enlace físico sólo durante la transmisión del paquete.
- Existen 2 tipos de CV
    - CVP: Circuito virtual permanente
    - CVT: Circuito virtual temporario
- CVP: no requiere fase de establecimiento o llamada virtual por ser un circuito permanente (punto a punto) entre ETDs.
- CVT: Requiere de la llamada virtual.
- El protocolo para uso de circuitos virtuales está establecido en la recomendación X.25 del CCITT. (existe confirmación de mensajes recibidos, paquetes perdidos, etc.)

Datagramas

El uso de datagrama permite balancear el tráfico de la subred gracias a que las rutas se pueden modificar a mitad de una conexión con lo cual no sufre las afectaciones como los circuitos virtuales que tienen que abortar.

El encaminamiento en redes de datagramas no se necesitan tablas con los circuitos virtuales, en este caso se almacenará una tabla que indica que salida deben utilizar para cada uno de los posibles IMP destinatarios.

Es un paquete autosuficiente (análogo a un telegrama) el cual contiene información suficiente para ser transportado a destino sin necesidad de, previamente, establecer un circuito.

No se provee confirmación de recepción por el destinatario, pero puede existir un aviso de no entrega por parte de la red.

Una alternativa al servicio de DATAGRAMA propuesto al CCITT, es la facilidad de selección rápida o Fast Select, la cual es aplicable en la llamada virtual ð CVT

Fast Select permite transmitir datos en el campo de datos del paquete de control que establece el circuito virtual. La respuesta confirma la recepción y termina el CV.

Asunto	**Datagramas**	**Circuito virtual**
Establecimiento	n/a	se requiere

Direccionamiento	de origen y destino en cada paquete	sólo número de CV
Información de estado	la sub red no tiene información de estado.	cada CV requiere una entrada en la tabla de sub red
Encaminamiento	cada paquete con ruta independiente.	todos los paquetes siguen la ruta establecida.
Efectos de falla en nodo	ninguno, perdida de paquetes	todos los CV a través del nodo con falla, terminan.
Control de congestión	difícil	fácil si un número suficiente de buffers son pre-asignados.
Complejidad	en la capa de transporte	en la capa de red
Adecuado para	servicios orientados a con y sin conexión.	servicios orientados a conexión.

Tabla 1. . Cuadro comparativo a nivel de subred

Protocolos y algoritmos de enrutamiento

Los protocolos de enrutamiento para la capa de red son usados para resolver peticiones de servicios de envío de paquetes de datos a través de diferentes redes de datos.

Para en análisis de enrutamiento a nivel de la capa de red se deben considerar tres aspectos importantes:

- Tablas de encaminamiento.
- Algoritmos de encaminamiento.
- Protocolos de encaminamiento

Tabla de enrutamiento

La función principal de un router es enviar un paquete hacia su red de destino, que es la dirección IP de destino del paquete. Para hacerlo, el router necesita buscar la información de enrutamiento almacenada en su tabla de enrutamiento.

Una tabla de enrutamiento es un archivo de datos en la RAM que se usa para almacenar la información de la ruta sobre redes remotas y conectadas directamente. La tabla de enrutamiento contiene asociaciones entre la red y el siguiente salto. Estas asociaciones le indican al router que un destino en particular se puede alcanzar mejor enviando el paquete hacia un router en particular, que representa el "siguiente salto" en el camino hacia el destino final. La asociación del siguiente salto también puede ser la interfaz de salida hacia el destino final.

La asociación entre la red y la interfaz de salida también puede representar la dirección de red de destino del paquete IP. Esta asociación ocurre en las redes del router conectadas directamente.

Una ***red conectada directamente*** es una red que está directamente vinculada a una de las interfaces del router. Cuando se configura una interfaz de router con una dirección IP y una máscara de subred, la interfaz pasa a ser un host en esa red conectada. La dirección de red y la

máscara de subred de la interfaz, junto con el número y el tipo de interfaz, se ingresan en la tabla de enrutamiento como una red ***conectada*** directamente. Cuando un router envía un paquete a un host, como por ejemplo un servidor Web, ese host está en la misma red que la red del router conectada directamente.

Una ***red remota*** es una red que no está directamente conectada al router. En otras palabras, una red remota es una red a la que sólo se puede llegar mediante el envío del paquete a otro router. Las redes remotas se agregan a la tabla de enrutamiento mediante el uso de un protocolo de ***enrutamiento dinámico*** o la ***configuración de rutas estáticas***. Las rutas dinámicas son rutas hacia redes remotas que fueron aprendidas automáticamente por el router utilizando un protocolo de enrutamiento dinámico. Las rutas estáticas son rutas hacia redes manualmente configuradas por un administrador de red.

Las siguientes analogías pueden ayudar a aclarar el concepto de ***rutas conectadas***, ***estáticas*** y ***dinámicas***:

Rutas conectadas directamente: Para visitar a un vecino, lo único que tiene que hacer es caminar por la calle donde vive. Esta ruta es similar a una ruta conectada directamente porque el "destino" está disponible directamente a través de su "***interfaz conectada***", la calle.

Rutas estáticas: Un tren siempre usa las mismas vías en una ruta específica. Esta ruta es similar a una estática porque la ruta hacia el destino es siempre la misma.

Rutas dinámicas: Al conducir un automóvil, usted puede elegir "***dinámicamente***" una ruta diferente según el tráfico, el clima y otras condiciones. Esta ruta es similar a una ruta dinámica porque puede elegir una nueva ruta en muchos puntos diferentes en su trayecto hacia el destino.

Cuando la tabla de enrutamiento incluye una ruta para una red remota, se incluye información adicional, como la ***métrica de enrutamiento*** y la ***distancia administrativa***.

En la figura siguiente se observa el resultado del comando ***route print***. El comando revela las redes de ***broadcast***, ***multicast***, ***loopback*** o de ***gateway*** por defecto que están configuradas o adquiridas.

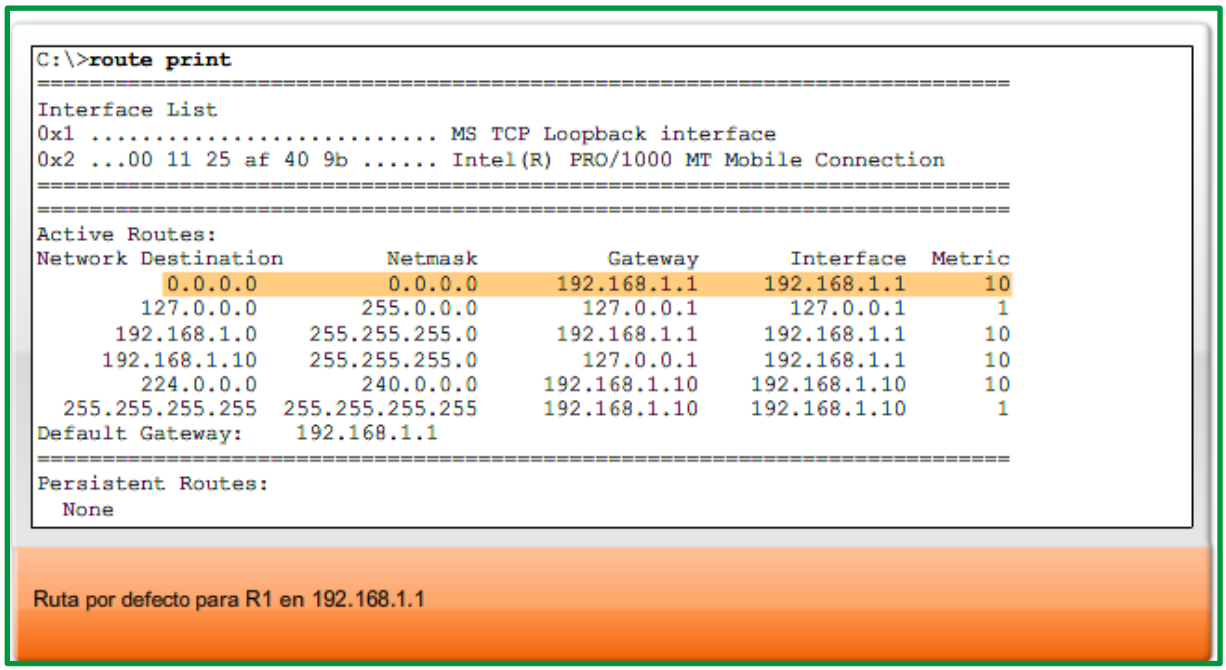


Figure 17. Datos de tabla de enrutamiento de un router

Enrutamiento estático

Las redes remotas se agregan a la tabla de enrutamiento mediante la configuración de rutas estáticas o la habilitación de un protocolo de enrutamiento dinámico. Cuando el IOS aprende sobre una red remota y la interfaz que usará para llegar a esa red, agrega la ruta a la tabla de enrutamiento siempre que la interfaz de salida esté habilitada.

Una ruta estática incluye la dirección de red y la máscara de subred de la red remota, junto con la dirección IP del router del siguiente salto o la interfaz de salida. Las rutas estáticas se indican con el código **S** en la tabla de enrutamiento, como se muestra en la figura.

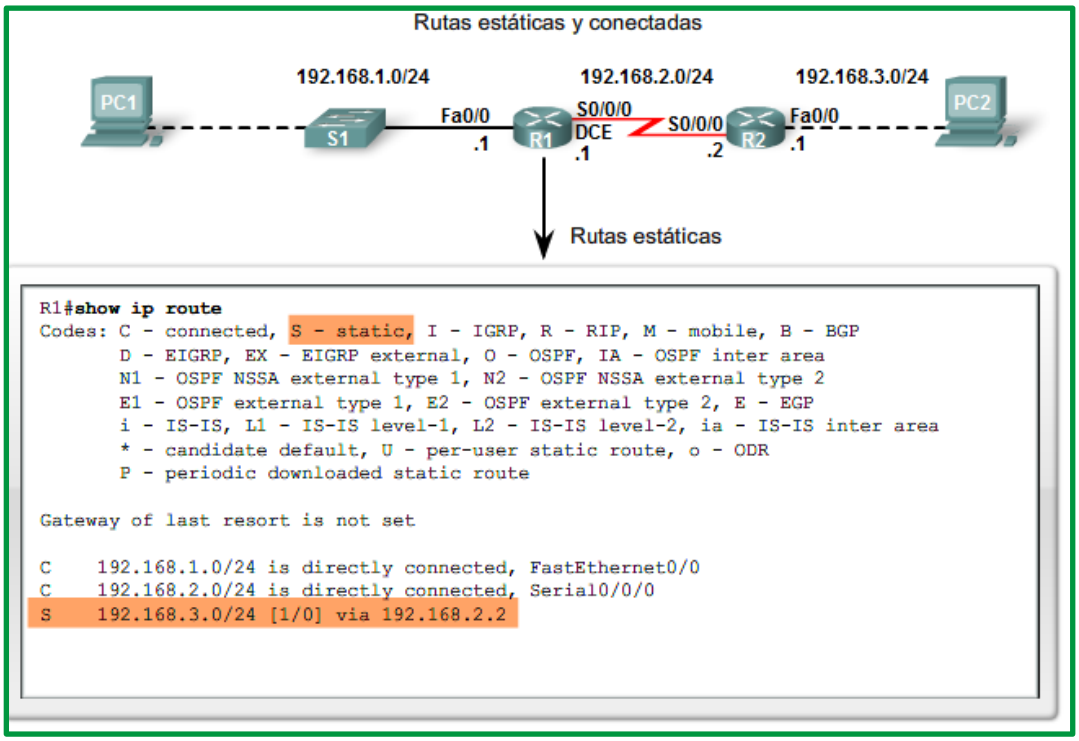


Figure 18. Ejemplo de ruta estática en un router

Cuándo usar rutas estáticas

Las rutas estáticas deben usarse en los siguientes casos:

- ***Una red está compuesta por unos pocos routers solamente***. En tal caso, el uso de un protocolo de enrutamiento dinámico no representa ningún beneficio sustancial. Por el contrario, el enrutamiento dinámico agrega más sobrecarga administrativa.
- ***Una red se conecta a Internet solamente a través de un único ISP***. No es necesario usar un protocolo de enrutamiento dinámico a través de este enlace porque el ISP representa el único punto de salida hacia Internet.
- ***Una red extensa está configurada con una topología hub-and-spoke***. Una topología hub-and-spoke comprende una ubicación central (el hub) y múltiples ubicaciones de sucursales (spokes), donde cada spoke tiene solamente una conexión al hub. El uso del enrutamiento dinámico sería innecesario porque cada sucursal tiene una única ruta hacia un destino determinado, a través de la ubicación central.

Generalmente, la mayoría de las tablas de enrutamiento contienen una combinación de rutas estáticas y rutas dinámicas. Sin embargo, como mencionamos antes, la tabla de enrutamiento debe contener primero las redes conectadas directamente que se usan para acceder a estas redes remotas antes de poder usar cualquier enrutamiento estático o dinámico.

Enrutamiento dinámico

Las redes remotas también pueden agregarse a la tabla de enrutamiento utilizando un protocolo de enrutamiento dinámico. En la figura siguiente, R1 ha aprendido automáticamente sobre la red

192.168.4.0/24 desde R2 a través del protocolo de enrutamiento dinámico, RIP (Routing Information Protocol). El RIP fue uno de los primeros protocolos de enrutamiento IP.

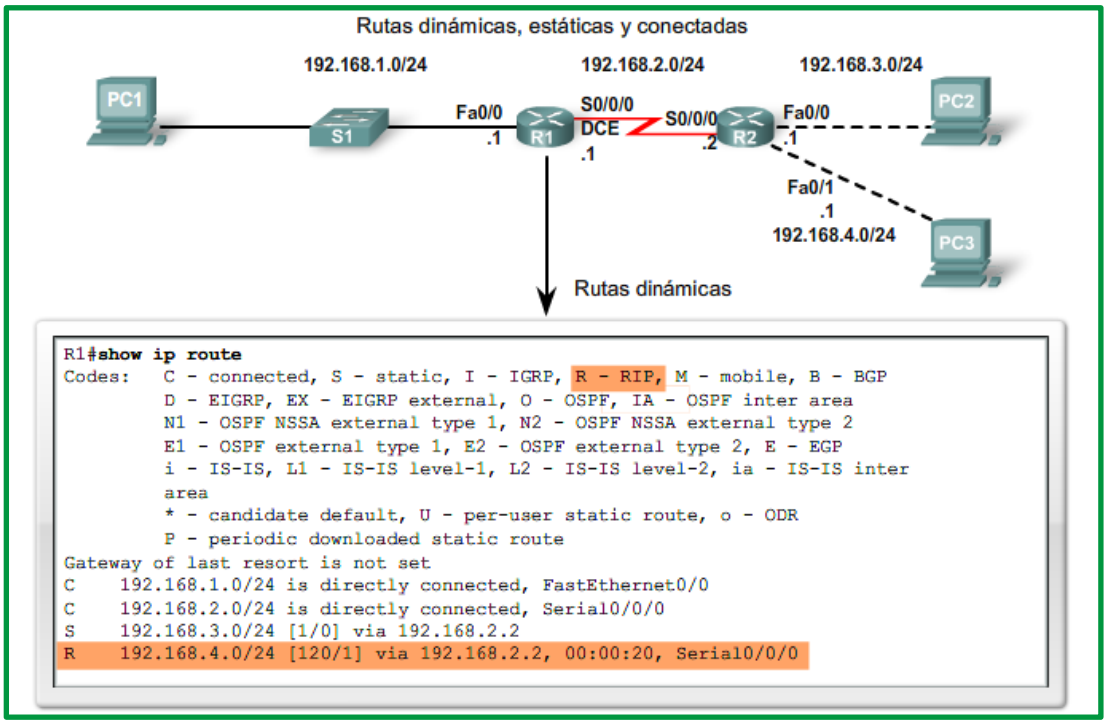


Figure 19. Ruta dinámica en un router aplicando protocolo RIP

Nota: La tabla de enrutamiento de R1 en la figura muestra que R1 ha aprendido sobre dos redes remotas: una ruta que usó el RIP dinámicamente y una ruta estática que se configuró en forma manual. Éste es un ejemplo de cómo las tablas de enrutamiento pueden contener rutas aprendidas dinámicamente y configuradas estáticamente y no necesariamente implica la mejor configuración para esta red.

Los routers, usan protocolos de enrutamiento dinámico para compartir información sobre el estado y la posibilidad de conexión de redes remotas. Los protocolos de enrutamiento dinámico ejecutan varias actividades, entre ellas:

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

Descubrimiento automático de redes

El descubrimiento de redes es la capacidad de un protocolo de enrutamiento de compartir información sobre las redes que conoce con otros routers que también están usando el mismo protocolo de enrutamiento. En lugar de configurar rutas estáticas hacia redes remotas en cada router, un protocolo de enrutamiento dinámico permite a los routers aprender automáticamente sobre estas redes a partir de otros routers. Estas redes, y la mejor ruta hacia

cada red, se agregan a la tabla de enrutamiento del router y se denotan como una red aprendida por un protocolo de enrutamiento dinámico específico.

Mantenimiento de las tablas de enrutamiento

Después del descubrimiento inicial de la red, los protocolos de enrutamiento dinámico actualizan y mantienen las redes en sus tablas de enrutamiento. Los protocolos de enrutamiento dinámico no sólo deciden acerca de la mejor ruta hacia diferentes redes, también determinan la mejor ruta nueva si la ruta inicial se vuelve inutilizable (o si cambia la topología). Por estos motivos, los protocolos de enrutamiento dinámico representan una ventaja sobre las rutas estáticas. Los routers que usan protocolos de enrutamiento dinámico automáticamente comparten la información de enrutamiento con otros routers y compensan cualquier cambio de topología sin requerir la participación del administrador de red.

Finalmente es importante señalar que los componentes básicos de la tabla de enrutamiento son la distancia administrativa, métricas y origen de la ruta.

Algoritmo de enrutamiento

El algoritmo de enrutamiento es la parte del software de la capa de red encargada de decidir la línea de salida por la que se transmitirá un paquete de entrada. Dentro del proceso de envió de datos a través de red desde el origen hacia su destino requieren, en tiempo y forma, algoritmos de ruteo, que se encarguen de escoger las rutas y las estructuras de datos que cumpla con ciertas propiedades que aseguren la eficiencia de su trabajo; estas propiedades son:

- Corrección,
- Estabilidad,
- Robustez,
- Equitatividad (balanceo),
- Optamización
- Adaptabilidad
- Sincorinización y
- Sencillez

Se consideran aspecto como:

- Si la subred usa datagramas entonces esta decisión debe hacerse cada vez que llega un paquete de datos de entrada, debido a que la mejor ruta podría haber cambiado desde la última vez.
- Si la subred utiliza circuitos virtuales internamente, las decisiones de enrutamiento se tomarán sólo al establecerse el circuito y los paquetes seguirán la ruta previamente establecida.

Los algoritmos de enrutamiento pueden agruparse en dos clases principales:

- **Algoritmos adaptables**: Basan sus decisiones de enrutamiento en mediciones, estimaciones de tráfico en la red y la topología descubierta.

- **Algoritmos no adaptables**: Basan sus decisiones de optar por una ruta de X a Y al calcular por adelantado, fuera de línea y se cargan en los router al iniciar la red. Éste procedimiento se llama enrutamiento estático.

Los algoritmos de enrutamiento se dividen en algoritmo estáticos y dinámicos.

Enrutamiento de inundación: Envía información a todos los nodos excepto aquella por la cual llego el paquete, la desventaja radica en la sobrecarga por transmisiones y recepción de información innecesarias. Aplicando estos algoritmos cada paquete de entrada se envía por cada una de las líneas de salida. Se caracteriza por su robustez y la rapidez en alcanzar un destino.

Enrutamiento por Shortest Path (camino más corto): Ampliamente aplicada, minimiza el número de saltos entre el origen y destino aplicando métricas basado en coste. Para medir la longitud de la ruta considera alguna métrica (número de saltos, la distancia física, el retraso de transmisión por un paquete de prueba, el ancho de banda, el tráfico promedio, el costo de comunicación, entre otros).

Enrutamiento basado en flujo: Consideran aspectos referente carga y congestión de enlaces, siempre hay una gran cantidad de tráfico entre un nodo A y un nodo B, ambos adyacentes, podría ser mejor enrutar (paquetes) el tráfico de ambos por caminos alternativos, aunque sea un poco más largos. La idea en que se basa el análisis es que, para una línea dada, si se conocen la capacidad y el flujo promedio, es posible calcular el retardo promedio de los paquetes en esa línea a partir de la teoría de colas. De los retardos promedio de todas las líneas, es directo el cálculo de un promedio ponderado por el flujo para obtener el retardo de paquete medio de la subred completa. El problema de enrutamiento se reduce entonces a encontrar el algoritmo de enrutamiento que produzca el retardo promedio mínimo para la subred

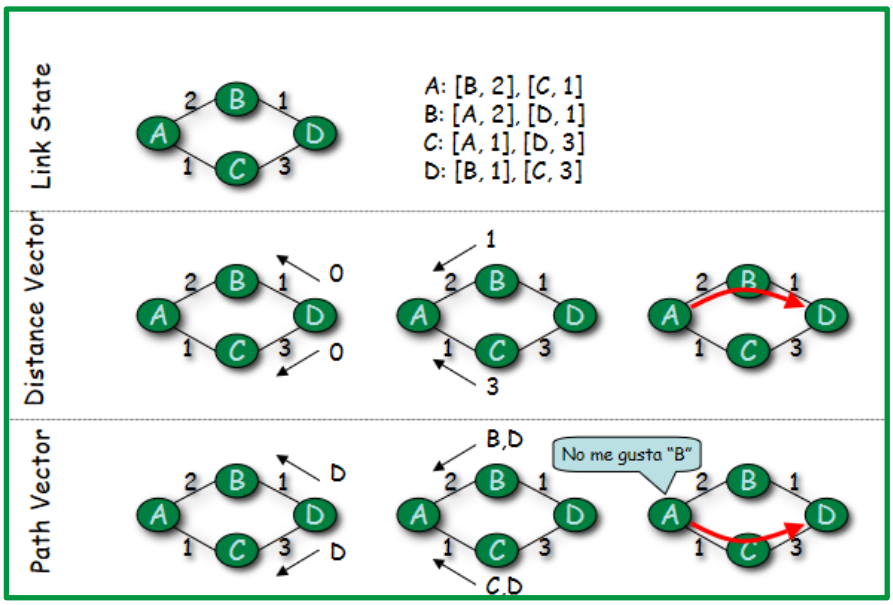


Figure 20. Tipo de algoritmos de enrutamiento

Algoritmos de Estado de enlace (Link State)

Los algoritmos de estado de enlace pueden describirse en cinco pasos:

1. Descubrir modos adyacentes y conocer sus direcciones de red
2. Medición del costo del de la línea.
3. Construcción de los paquetes de estado enlace.
4. Distribución de los paquetes de estado enlace.
5. Cálculo de nuevas rutas.

Algoritmo de Dijkstra.

Halla el camino de mínima distancia entre un nodo origen (o raíz) y cualquier otro nodo de la red.

La idea es construir el camino de distancia más corta en orden de longitud de camino creciente, es decir, se va iterando con la distancia, seleccionando en cada caso el nodo más cercano.

Notación:

C(x,y): coste de enlace entre los nodos x e y

D(v): valor actual de la ruta desde el origen al destino v.

P(v): nodo predecesor en la ruta del origen al destino v.

N': conjunto de nodo cuyo camino de coste mínimo se conoce.

Inicialización
N'= {u}
for todo nodo v
If v es adyacente a u **then**
D(v) = ∞
else D(v) = ∞
Bucle:
Repeat
Encontrar w e N' tal que D(w) es un mínimo
Añadir w a N'
Actualizar D(v) ∀ v ∉ N' y adyacente a w:
D(v)= min (D(v))), D(w) + c (w,v))
Until todos los nodos están en N'

Ejemplificación de aplicación del algoritmo de **Dijkstra,** se requiere establecer las rutas para la siguiente topología.

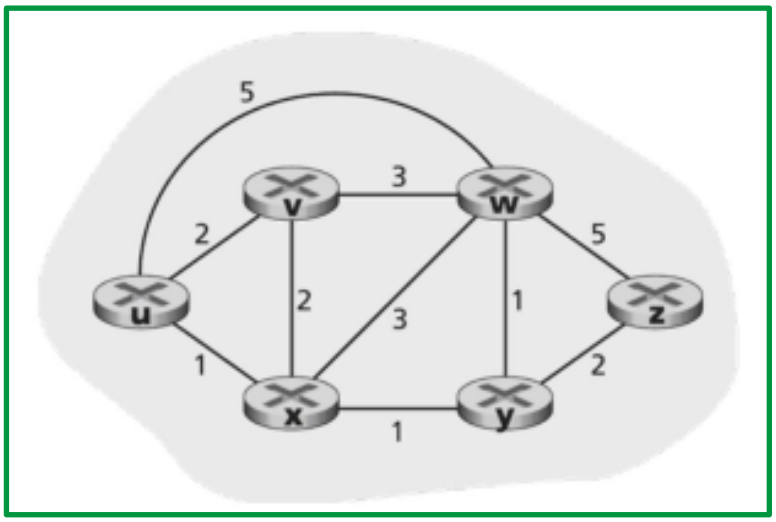


Figure 21. Topología para aplicar ejemplo de algoritmo de Dijkstra

PASOS	N'	D(v),p(v)	D(w),p(w)	D(x),p(x)	D(y),p(y)	D(z),p(z)
0	u	2,u	5,u	1,u	∞	∞
1	ux	2,u	4,x		2,x	∞
2	uxy	2,u	3,y			4,y
3	uxyv		3,y			4,y
4	uxyvw					4,y
5	uxyvwz					

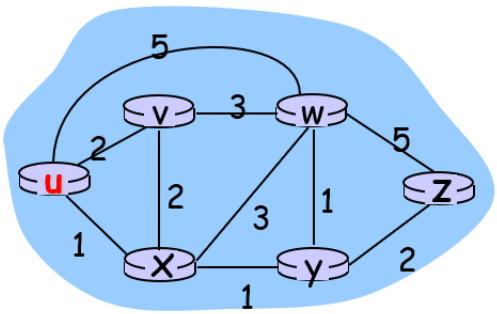


Figure 22. Figure 22. Ejemplo algoritmo de Dijkstra
Fuente: https://www.youtube.com/watch?v=FTLfOUZuurU

Árbol de rutas mínimas desde *u*:

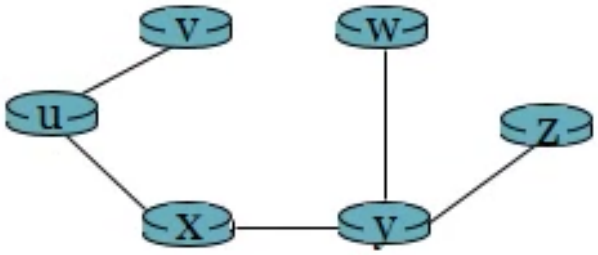


Tabla de reenvío resultante desde *u*:

destino	enlace
v	(*u*,*v*)
x	(*u*,*x*)
y	(*u*,*x*)
w	(*u*,*x*)
z	(*u*,*x*)

Figure 23. Rutas resultantes de ejemplo

Algoritmo del camino más ancho. Aproximación basada en Dijsktra

Algorithm 2.8 Widest path algorithm, computed at node i (Dijkstra based).

1. Discover the list of nodes in the network, $\mathcal{N}$ and available bandwidth of link k-m, $b^i_{km}(t)$, as known to node i at the time of computation, t.
2. Initially, consider only source node i in the set of nodes considered, i.e., $\mathcal{S} = \{i\}$; mark the set with all the rest of the nodes as $\mathcal{S}'$. Initialize

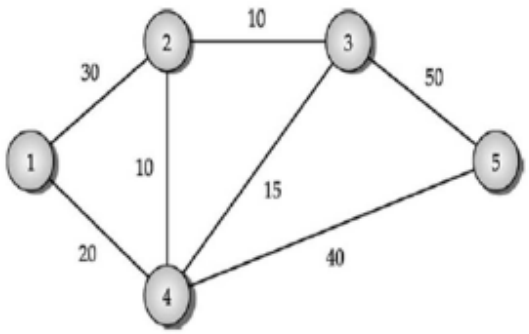
$$\underline{B}_{ij}(t) = b^i_{ij}(t) \quad \text{for all} \quad j \in \mathcal{S}'. \tag{2.7.1}$$

3. Identify a neighboring node (intermediary) k not in the current list $\mathcal{S}$ with the maximum bandwidth from node i, i.e., find $k \in \mathcal{S}'$ such that $\underline{B}_{ik}(t) = \max_{m \in \mathcal{S}'} \underline{B}_{im}(t)$
   Add k to the list $\mathcal{S}$, i.e., $\mathcal{S} = \mathcal{S} \cup \{k\}$
   Drop k from $\mathcal{S}'$, i.e., $\mathcal{S}' = \mathcal{S}' \backslash \{k\}$.
   If $\mathcal{S}'$ is empty, stop.
4. Consider nodes in $\mathcal{S}'$ to update maximum bandwidth path, i.e.,
   for $j \in \mathcal{S}'$

$$\underline{B}_{ij}(t) = \max\{\underline{B}_{ij}(t), \min\{\underline{B}_{ik}, b^i_{kj}(t)\}\}. \tag{2.7.2}$$

   Go to Step 3.

Figure 24. Algoritmo de ruta más amplia



Para el nodo 2:

$\underline{B}_{13} = \max\{\underline{B}_{13}, \min\{B_{12}, b_{23}\}\} = \max\{0, \min\{30, 10\}\} = 10$ // use 1-2-3

$\underline{B}_{14} = \max\{\underline{B}_{14}, \min\{B_{12}, b_{24}\}\} = \max\{20, \min\{30, 10\}\} = 20$ // stay on 1-2

$\underline{B}_{15} = \max\{\underline{B}_{15}, \min\{B_{12}, b_{25}\}\} = \max\{0, \min\{30, 0\}\} = 0$ // no change

Para el nodo 4:

$\underline{B}_{13} = \max\{\underline{B}_{13}, \min\{B_{14}, b_{43}\}\} = \max\{10, \min\{20, 15\}\} = 15$ // use 1-4-3

$\underline{B}_{15} = \max\{\underline{B}_{15}, \min\{B_{14}, b_{45}\}\} = \max\{0, \min\{20, 40\}\} = 20$ // use 1-4-5

Iteration	List, $\mathcal{S}$	$\underline{B}_{12}$	Path	$\underline{B}_{13}$	Path	$\underline{B}_{14}$	Path	$\underline{B}_{15}$	Path
1	{1}	30	1-2	0	–	20	1-4	0	–
2	{1, 2}	30	1-2	10	1-2-3	20	1-4	0	–
3	{1, 2, 4}	30	1-2	15	1-4-3	20	1-4	20	1-4-5
4	{1, 2, 4, 3}	30	1-2	15	1-4-3	20	1-4	20	1-4-5
5	{1, 2, 4, 3, 5}	30	1-2	15	1-4-3	20	1-4	20	1-4-5

Figure 25. Ejemplo de algoritmo de ruta más amplia

Algoritmo de distancia o VD (Distance Vector).

Conocido también como Bellman-Ford, algoritmo dinámico que se adapta a los cambios en las topologías de la red; cada router mantiene una tabla de enrutamiento en la cual hay una entrada por cada nodo destino en la red.

Los algoritmos de vector-distancia crean las tablas de encaminamiento teniendo en cuenta la distancia para alcanzar el destino. Para el cálculo de la distancia al destino se utiliza una métrica basada en una o más de las siguientes características de la ruta:

- **Número de saltos**: Cantidad de routers que un paquete debe atravesar hasta llegar a su destino.
- **Ancho de banda**: Capacidad de transmisión de datos de un enlace.
- **Retardo**: Cantidad de tiempo requerido para transportar un paquete de datos por cada enlace desde el origen hasta el destino.
- **Carga**: Cantidad de actividad en un recurso de red, tal como un router o un enlace.
- **Fiabilidad**: Índice de error de cada enlace en la red.
- **Coste**: Valor arbitrario asignado por el administrador de red y basado en el ancho de banda, coste monetario, importancia de los datos, etc.

En este aspecto, para existe un proceso dinámico de actualización, cada nodo recibe de sus vecinos sus respectivas tablas de enrutamiento, las compara con la suya para calcular su nueva tabla de enrutamiento misma que es compartida a los nodos vecinos después del proceso de actualización.

Algoritmo de Bellman

Se trata de un procedimiento sistemático basado en las fórmulas de recurrencia de Bellman, que es fácilmente programable y que da las soluciones óptimas para alcanzar un vértice final o un grupo de vértices finales.

Supongamos que el grafo contiene n vértices. Se comienza por definir la matriz C= (c(x, y)) en donde c(x, y) es el coste de la transición x y en una etapa, se pone c(x, y)= +¥ si dicha transición no es posible. Denotemos por:

V(x): Función de retorno óptima.

Vk(x): Función que da el coste mínimo para alcanzar el vértice final (o vértices finales), desde el vértice x, en k etapas o menos.

El algoritmo de Bellman y Kalaba desarrollado en cuatro pasos es:

- **Paso 1**: (k=0)

$$V_0(x) = \begin{cases} 0 & si\ x\ es\ un\ vértice\ final \\ +\infty & en\ otro\ caso \end{cases}$$

$$Paso\ 2\text{: } (k \rightarrow k+1)\text{: } V_k(x) = \min \{ \min_{y \neq x} \{c(x,y) + V_{k-1}(y)\}, V_{k-1}(x) \}$$

- **Paso 3**: Comparamos Vk (x) con Vk-1(x). Si difieren para algún vértice x, ir al paso 2; en caso contrario, los valores obtenidos son los óptimos, por lo que tenemos los valores de la función de retorno optimal V(x) = Vk (x) = coste mínimo para alcanzar desde x el vértice o los vértices finales.
- **Paso 4:** (Reconstrucción de las cadenas o caminos óptimos) Desde un vértice x se pasa al vértice y que satisfaga la ecuación V(x) = c(x, y) + V(y).

Ejemplificación: Aplicar el algoritmo anterior al grafo de la figura para encontrar los caminos óptimos que conducen al vértice 6.

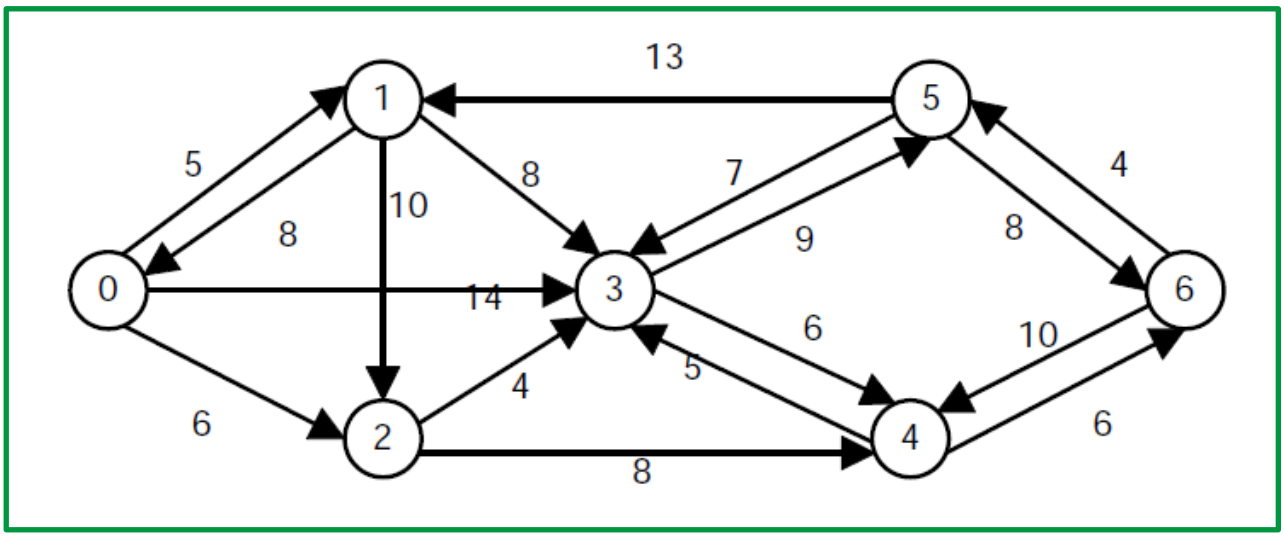


Figure 26. Ejemplificación de algoritmo Bellman

Aplicando el algoritmo y recogiendo los pasos en una tabla se obtiene lo siguiente:

	Vértices						
k	0	1	2	3	4	5	6
0	∞	∞	∞	∞	∞	∞	0
1	∞	∞	∞	∞	6	8	0
2	∞	∞	14	12	6	8	0
3	20	20	14	12	6	8	0
4	20	20	14	12	6	8	0

Figure 27. Tabla de datos aplicando los pasos del algoritmo de Bellman

Cada fila de la tabla con k³1 se construye a partir de la fila anterior sin más que aplicar lo establecido en el paso 2. En el momento en que se repiten los valores de dos filas consecutivas, se detiene el proceso y esos valores finales son precisamente los de la función de retorno optima V(x). La reconstrucción de los caminos óptimos para este ejemplo conduce a la solución mostrada en la siguiente gráfica:

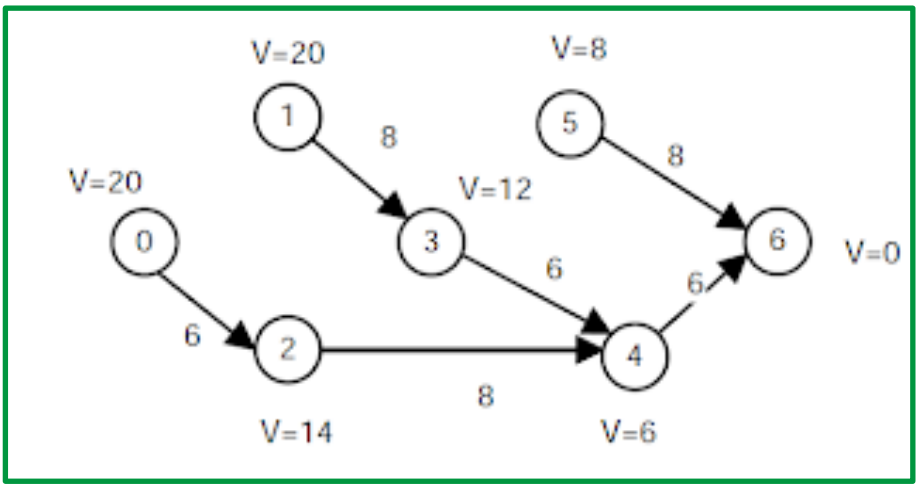


Figure 28. Solución óptima para alcanzar el vértice 6

Ejemplo:

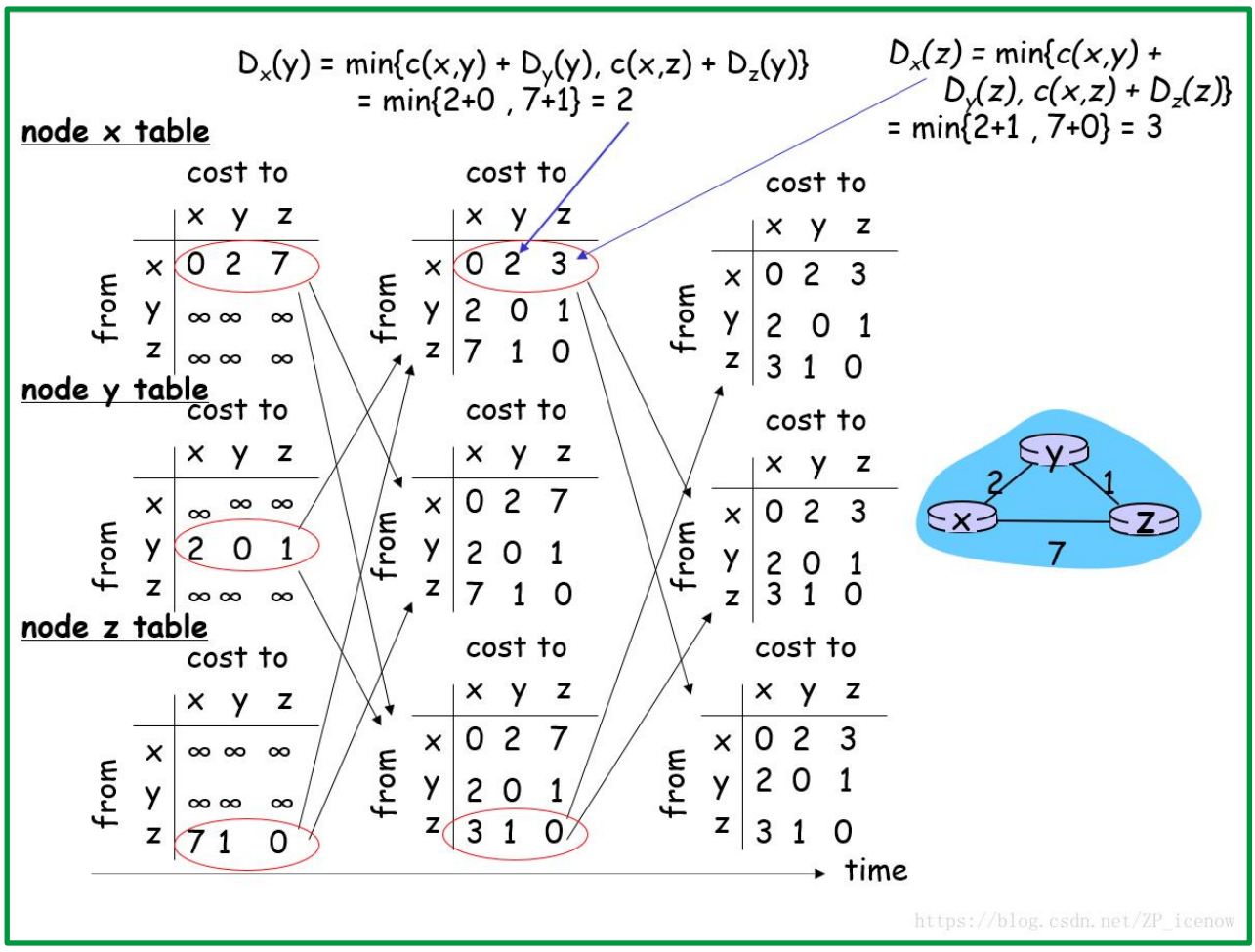


Figure 29. Ejemplo a nivel de enrutamiento de aplicación de algoritmo de Bellman

Protocolos de enrutamiento IP

Existen varios protocolos de enrutamiento dinámico para IP. Éstos son algunos de los protocolos de enrutamiento dinámico más comunes para el enrutamiento de paquetes IP:

- **RIP (Routing Information Protocol)**. Un protocolo de enrutamiento interior vector distancia.
    - El protocolo RIP, Routing information Protocol (Protocolo de información de enrutamiento), es un protocolo de enrutamiento de vector-distancia, en uso en miles de redes de todo el mundo. RIP se basa en un estándar abierto, descrito en el RFC 1058 y RFC-2453, de fácil implementación, aunque carece de la capacidad y de las características de los protocolos de enrutamiento más avanzados.
    - RIP ha evolucionado a lo largo de los años desde la versión v.1 hasta la version v.2. La versión v.1 realiza encaminamiento classfull o con clase mientras que la versión v.2 lo hace classless o sin clase. Un protocolo de encaminamiento classfull o con clase es aquel que no admite la utilización de máscaras diferentes a las de la propia clase. En cambio, un protocolo de encaminamiento classless o sin clase puede utilizar máscaras diferentes. Por tanto, la versión v.2 permite trabajar con subredes
    - Además, la versión v.2 de RIP tiene capacidad para transportar mayor información relativa al enrutamiento de paquetes y mecanismos de autenticación para la seguridad de origen al hacer actualizaciones de las tablas.
    - En principio, el protocolo RIP divide las máquinas participantes en activas o pasivas. Sólo los routers pueden ejecutar RIP en modo activo, de modo que los equipos deberán ejecutar RIP en modo pasivo. Los routers activos notifican sus rutas a los otros routers; los equipos pasivos listan y actualizan sus rutas basándose en estas notificaciones. Los routers envían cada 30 segundos un mensaje de difusión con las actualizaciones de encaminamiento a sus vecinos.
    - Cuando un router crea una ruta en su tabla, inicia un temporizador para tal ruta. Este tiempo debe iniciarse cada vez que el router recibe otro mensaje RIP anunciando la ruta. La ruta queda invalidada si transcurren 180 segundos sin que el router haya recibido nuevamente una notificación.
    - El protocolo RIP utiliza como métrica para la selección de rutas el número de saltos; es decir, el número de routers que un paquete encontrará a su paso a lo largo de una ruta desde un nodo origen dado hacia un destino.
    - Para evitar que se produzcan bucles de enrutamiento infinitos en la red, RIP fija un límite en el número de saltos permitido en una ruta desde su origen hasta su destino. El número máximo de saltos permitido en una ruta es de 15. Cuando un router recibe una actualización de enrutamiento que contiene una entrada nueva o cambiada, el valor de la métrica aumenta en 1, para incluir el salto correspondiente a sí mismo. Si este incremento hace que la métrica supere la cifra de 15, se considera que es infinita y la red de destino se considera fuera de alcance y los paquetes son desechados. Esto hace que RIP sea un protocolo que solamente es adecuado para redes pequeñas. En una red grande, el administrador debe dividirla en secciones o utilizar un protocolo alternativo.
    - Los routers RIP conservan sólo la mejor ruta hacia un destino, pero pueden conservar más de una ruta al mismo destino si el coste de todas es igual hasta que aparezca una ruta nueva con un coste menor.

- Al igual que otros protocolos de enrutamiento, RIP implementa diferentes técnicas (cuenta al infinito, horizonte dividido, actualización inversa, temporizadores de espera, actualizaciones generadas por eventos, …) para reducir los bucles de enrutamiento y prevenir la propagación de información de enrutamiento errónea.
- RIP tiene una convergencia lenta debido a que los temporizadores de espera (180 segundos) hacen que los mensajes de actualización de encaminamiento se difundan lentamente a través de la red. Es posible reducir el temporizador de espera, para agilizar la convergencia, pero esto se debe hacer con cautela.

- **IGRP (Interior Gateway Routing Protocol).** Enrutamiento interior vector distancia desarrollado por Cisco.

- **EIGRP (Enhanced Interior Gateway Routing Protocol)**. el protocolo avanzado de enrutamiento interior vector distancia desarrollado por Cisco.
  - EIGRP se lanzó originalmente en 1992 como un protocolo exclusivo disponible solamente en los dispositivos de Cisco. En 2013, Cisco cedió una funcionalidad básica de EIGRP como estándar abierto al IETF, como una RFC informativa.
  - El algoritmo de actualización por difusión (DUAL), constituye el centro del protocolo de routing. DUAL garantiza rutas de respaldo y sin bucles en todo el dominio de routing.
  - Las adyacencias de vecinos se usan para rastrear el estado de esos vecinos.
  - El protocolo de transporte confiable (RTP) es exclusivo de EIGRP y se encarga de la entrega de los paquetes EIGRP a los vecinos.
  - En lo que respecta a sus actualizaciones, en EIGRP se utilizan los términos “parcial” y “limitada”. A diferencia de RIP, EIGRP no envía actualizaciones periódicas, y las entradas de ruta no vencen.
  - EIGRP admite balanceo de carga de mismo costo y balanceo de carga con distinto costo, lo que permite a los administradores distribuir mejor el flujo de tráfico en sus redes.
  - EIGRP tiene la capacidad para enrutar varios protocolos diferentes, incluidos IPv4 e IPv6, mediante el uso de módulos dependientes de protocolo (PDM).

- **OSPF (Open Shortest Path First**). Protocolo de enrutamiento interior de link-state.
  El protocolo OSPF, Open Short Path First (Primero la ruta más corta), es uno de los protocolos del estado-enlace más importantes. Este protocolo estándar descrito en el RFC 2328 se caracteriza por:
  - Realizar la actualización de la información de encaminamiento según el algoritmo de estado-enlace.
  - Utilizar el algoritmo SPF (Short Path First) para calcular el costo más bajo hasta un destino.
  - Poder determinar la red destino del mensaje utilizando máscaras diferentes a la máscara por defecto de la clase a la que pertenece el equipo destino. Es un protocolo classless o sin clases
  - Soportar tipos de servicio. Los administradores de red pueden instalar múltiples rutas hacia un destino dado, una por cada tipo de servicio.

- Proporcionar balanceo de carga entre rutas de igual peso. Si un administrador especifica múltiples rutas hacia un destino con el mismo coste, el protocolo OSPF distribuye el tráfico entre todas las rutas de la misma manera. Esta es una diferencia importante con respecto a RIP que calcula una sola ruta para cada destino.
- Permitir la partición en áreas y sistemas autónomos para el encaminamiento independiente en cada área. Los anuncios del estado de los enlaces se envían a todos los routers de un área.
- Realizar la localización automática de routers vecinos.
- Permitir la propagación de rutas aprendidas de fuentes externas.
- Propagar entre los enlaces las tablas de encaminamiento sólo cuando se detecta un cambio en la configuración de la red, ya que cuando se realizan actualizaciones, se produce un gran volumen de tráfico en la red.

El protocolo OSPF supera las limitaciones de otros protocolos; como, por ejemplo, RIP que converge lentamente y a veces elige rutas lentas porque no tiene en cuenta aspectos críticos como el ancho de banda a la hora de determinar la ruta.

- **IS-IS (Intermediate System-to-Intermediate System).** Protocolo de enrutamiento interior de link-state.
- **BGP (Border Gateway Protocol).** Protocolo de enrutamiento exterior vector ruta, definido en RFC-1771
  - Conocido también como dominio de enrutamiento, es un conjunto de routers que se encuentran bajo una administración común.
  - BGP dirige paquetes entre sistemas autónomos (AS): redes administradas por una sola empresa o proveedor de servicios. El tráfico que se enruta dentro de una única red AS se conoce como BGP interno o iBGP. Más a menudo, BGP se utiliza para conectar un AS a otros sistemas autónomos, y luego se denomina BGP externo o eBGP.

Sabías que. - El IGRP es un protocolo de enrutamiento heredado que ha sido reemplazado por el EIGRP. El IGRP y el EIGRP son protocolos de enrutamiento patentados por Cisco, mientras que todos los demás protocolos de enrutamiento enumerados son protocolos estándares, no patentados.

Recuerde que. - En la mayoría de los casos, los routers contienen una combinación de rutas estáticas y rutas dinámicas en las tablas de enrutamiento.

LA METRICA Y MEJOR RUTA

Métricas.

En algunos casos, un protocolo de enrutamiento obtiene información sobre más de una ruta hacia el mismo destino. Para seleccionar el mejor camino, el protocolo de enrutamiento debe

poder evaluar y diferenciar entre las rutas disponibles. Para tal fin, se usa una métrica. Una métrica es un valor utilizado por los protocolos de enrutamiento para asignar costos a fin de alcanzar las redes remotas. La métrica se utiliza para determinar qué ruta es más preferible cuando existen múltiples rutas hacia la misma red remota. Cada protocolo de enrutamiento usa su propia métrica.

Las métricas utilizadas en los protocolos de enrutamiento IP incluyen:

- ✓ **Conteo de saltos**: Una métrica que cuenta la cantidad de routers que un paquete tiene que travesar en la red para alcanzar su destino.
- ✓ **Ancho de banda**: Selecciona rutas al considerar aquellas que tenga un mayor ancho de banda
- ✓ **Carga**: Considera la utilización de un enlace determinado en función al tráfico de la red.
- ✓ **Retardo**: Considera el tiempo que un paquete tarda en atravesar una ruta
- ✓ **Confiabilidad**: Evalúa la probabilidad de una falla de enlace calculada a partir del conteo de errores de la interfaz o fallas de enlaces previas.
- ✓ **Costo**: Un valor determinado por IOS o por el administrador de red para indicar la preferencia de una ruta.
- ✓ **MTU**: Unidad máxima de transmisión que pueden ser aceptadas por todos los enlaces de la ruta.
- ✓ **Pulsos:** Retraso en un enlace de datos usando pulsos de reloj de PC.

En la siguiente tabla se enumeran los protocolos dinámicos comunes y sus métricas.

Tabla 1. Métricas de protocolos de enrutamiento

Protocolo de enrutamiento	Métrica
Routing Information Protocol (RIP)	• La métrica es «recuento de saltos». • Cada router a lo largo de una ruta agrega un salto al recuento de saltos. • Se permite un máximo de 15 saltos.
Open Shortest Path First (OSPF)	• La métrica es «costo», que es la basada en la Basado en el ancho de banda acumulado de origen a destino • A los enlaces más rápidos se les asignan costos más bajos en comparación con los más lentos (mayor costo).
Enhanced Interior Gateway Routing Protocol (EIGRP)	• Calcula una métrica basada en los valores de ancho de banda y retraso (delay) más lentos. • También podría incluir carga y fiabilidad en la métrica cálculo

La mayoría de los protocolos de ruteo tienen algoritmos y estructuras de métricas que no son compatibles con otros protocolos. En una red con múltiples protocolos de ruteo, el intercambio de la información de rutas y la capacidad para seleccionar la mejor trayectoria a través de los protocolos múltiples son fundamentales.

La distancia administrativa es un valor que utilizan los routers para seleccionar la mejor trayectoria cuando hay dos o más rutas diferentes hacia el mismo destino desde dos protocolos de ruteo distintos. La distancia administrativa define la confiabilidad de un protocolo de ruteo. Se da prioridad a cada protocolo de ruteo en orden de mayor a menor confiabilidad (credibilidad) usando un valor de distancia administrativa.

Seleccionar la Mejor Trayectoria

La distancia administrativa es el primer criterio que un router utiliza para determinar qué protocolo de ruteo utilizar si dos protocolos proporcionan información de ruta para el mismo destino. La distancia administrativa mide la fiabilidad de la fuente de la información de ruteo. La distancia administrativa tiene importancia local solamente y no se publica en actualizaciones de ruteo.

Sabías que. - Cuanto más bajo sea el valor de la distancia administrativa, más confiable será el protocolo. Por ejemplo, si un router recibe una ruta a cierta red de Open Shortest Path First (OSPF) (distancia administrativa predeterminada: 110) y de Interior Gateway Routing Protocol (IGRP) (distancia administrativa predeterminada: 100), el router optará por IGRP porque es más confiable. Esto significa que el router agrega la versión de la ruta de IGRP a la tabla de ruteo.

Si se pierde la fuente de la información derivada de IGRP (debido a un corte en el suministro eléctrico, por ejemplo), el software utiliza la información derivada de OSPF hasta que reaparezca la información derivada de IGRP.

En esta tabla se incluyen los valores predeterminados de la distancia administrativa de los protocolos:

Tabla 2. Tabla del valor de distancia predeterminada

Fuente de la Ruta	Valores Predeterminados de la Distancia
Interfaz conectada	0
Static ruta	1
Ruta de resumen del Enhanced Interior Gateway Routing Protocol (EIGRP)	5
Border Gateway Protocol (BGP) externo	20
EIGRP Interno	**90**
IGRP	100
OSPF	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
On-Demand Routing (ODR)	160
EIGRP externo	170
BGP interno	200
Unknown*	255

*Si la distancia administrativa es de 255, el router no cree en la fuente de esa ruta y no instala la ruta en la tabla de ruteo.

En ocasiones, cuando se utiliza la redistribución de ruta, se debe modificar la distancia administrativa de un protocolo para que este adquiera prioridad. Por ejemplo, si desea que el router seleccione rutas aprendidas de RIP (valor predeterminado: 120) en lugar de rutas aprendidas de IGRP (valor predeterminado: 100) para el mismo destino, debe aumentar la distancia administrativa de IGRP a 120+ o disminuir la distancia administrativa de RIP a un valor inferior a 100.

Usted puede modificar la distancia administrativa de un protocolo a través del comando en el modo de subconfiguración del proceso de ruteo. El comando especifica que la distancia administrativa está asignada a las rutas aprendidas de un protocolo de ruteo en particular. Por lo general, debe utilizar este procedimiento cuando emigra la red a partir de un protocolo de ruteo a otro y este último tiene una distancia administrativa más alta. Sin embargo, un cambio en la distancia administrativa puede dar lugar a loops de ruteo y a agujeros negros. Por lo tanto, tenga cuidado si cambia la distancia administrativa.

Aquí hay un ejemplo que muestra dos routers, R1 y R2, conectados a través de Ethernet. Las interfaces Loopback de los routers también se publican con RIP e IGRP en ambos routers. Puede observar que se prefieren las rutas IGRP antes que las rutas RIP en la tabla de ruteo porque la distancia administrativa es de 100.

La mejor ruta

La identificación de la mejor ruta de un router implica la evaluación de múltiples rutas hacia la misma red de destino y la selección de la ruta óptima o "la más corta" para llegar a esa red. Cuando existen múltiples rutas para llegar a la misma red, cada ruta usa una interfaz de salida diferente en el router para llegar a esa red. La mejor ruta es elegida por un protocolo de enrutamiento en función del valor o la métrica que usa para determinar la distancia para llegar a esa red. Algunos protocolos de enrutamiento, como RIP, usan un conteo de saltos simple, que consiste en el número de routers entre un router y la red de destino. Otros protocolos de enrutamiento, como OSPF, determinan la ruta más corta al analizar el ancho de banda de los enlaces y al utilizar dichos enlaces con el ancho de banda más rápido desde un router hacia la red de destino.

Los protocolos de enrutamiento dinámico generalmente usan sus propias reglas y métricas para construir y actualizar las tablas de enrutamiento. Una métrica es un valor cuantitativo que se usa para medir la distancia hacia una ruta determinada. La mejor ruta a una red es la ruta con la métrica más baja. Por ejemplo, un router preferirá una ruta que se encuentra a 5 saltos antes que una ruta que se encuentra a 10 saltos.

El objetivo principal del protocolo de enrutamiento es determinar las mejores trayectorias para cada ruta a fin de incluirlas en la tabla de enrutamiento. El algoritmo de enrutamiento genera un valor, o una métrica, para cada ruta a través de la red. Las métricas se pueden calcular sobre la base de una sola característica o de varias características de una ruta. Algunos protocolos de

enrutamiento pueden basar la elección de la ruta en varias métricas, combinándolas en un único valor métrico. Cuanto menor es el valor de la métrica, mejor es la ruta.

Comparación del conteo de saltos y la métrica del ancho de banda

Dos de las métricas que usan algunos protocolos de enrutamiento dinámicos son:

- **Conteo de saltos**: Cantidad de routers que debe atravesar un paquete antes de llegar a su destino. Cada router es igual a un salto. Un conteo de saltos de cuatro indica que un paquete debe atravesar cuatro routers para llegar a su destino. Si hay múltiples rutas disponibles hacia un destino, el protocolo de enrutamiento (por ejemplo RIP) selecciona la ruta que tiene el menor número de saltos.
- **Ancho de banda**: Es la capacidad de datos de un enlace, a la cual se hace referencia a veces como la velocidad del enlace. Por ejemplo, la implementación del protocolo de enrutamiento OSPF de Cisco utiliza como métrica el ancho de banda. La mejor ruta hacia una red se determina según la ruta con una acumulación de enlaces que tienen los valores de ancho de banda más altos, o los enlaces más rápidos.

Cuando se usa el conteo de saltos como métrica, la ruta resultante a veces puede ser subóptima. Por ejemplo, considere la red que se muestra en la figura. Si RIP es el protocolo de enrutamiento utilizado por los tres routers, entonces R1 utilizará la ruta subóptima hacia R3 para llegar a la PC2 porque esta ruta tiene menos saltos. No se tiene en cuenta el ancho de banda. Sin embargo, si se usa OSPF como protocolo de enrutamiento, entonces R1 elegirá la ruta basándose en el ancho de banda. Los paquetes podrán llegar a destino antes utilizando los dos enlaces T1 más rápidos, en comparación con el enlace único de 56 Kbps más lento.

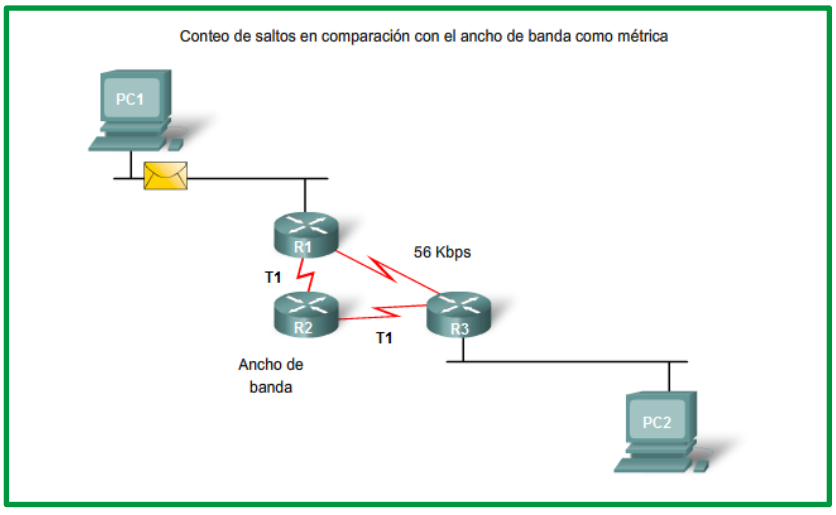


Figure 30. Comparación de métricas de protocolos de enrutamiento

Determinación de ruta

El envío de paquetes supone dos funciones:

- Función de determinación de ruta
- Función de conmutación

La función de determinación de ruta es el proceso según el cual el router determina qué ruta usar cuando envía un paquete. Para determinar la mejor ruta, el router busca en su tabla de enrutamiento una dirección de red que coincida con la dirección IP de destino del paquete.

El resultado de esta búsqueda es una de tres determinaciones de ruta:

- **Red conectada directamente**: Si la dirección IP de destino del paquete pertenece a un dispositivo en una red que está directamente conectado a una de las interfaces del router, ese paquete se envía directamente a ese dispositivo. Esto significa que la dirección IP de destino del paquete es una dirección host en la misma red que la interfaz de este router.
- **Red remota**: Si la dirección IP de destino del paquete pertenece a una red remota, entonces el paquete se envía a otro router. Las redes remotas sólo se pueden alcanzar mediante el envío de paquetes a otro router.
- **Sin determinación de ruta**: Si la dirección IP de destino del paquete no pertenece ya sea a una red conectada o remota, y si el router no tiene una ruta por defecto, entonces el paquete se descarta. El router envía un mensaje ICMP de destino inalcanzable a la dirección IP de origen del paquete.

En los primeros dos resultados, el router vuelve a encapsular el paquete IP en el formato de la trama de enlace de datos de Capa 2 de la interfaz de salida. El tipo de interfaz determina el tipo de encapsulación de Capa 2. Por ejemplo, si la interfaz de salida es FastEthernet, el paquete se encapsula en una trama de Ethernet. Si la interfaz de salida es una interfaz serial configurada para PPP, el paquete IP se encapsula en una trama PPP.

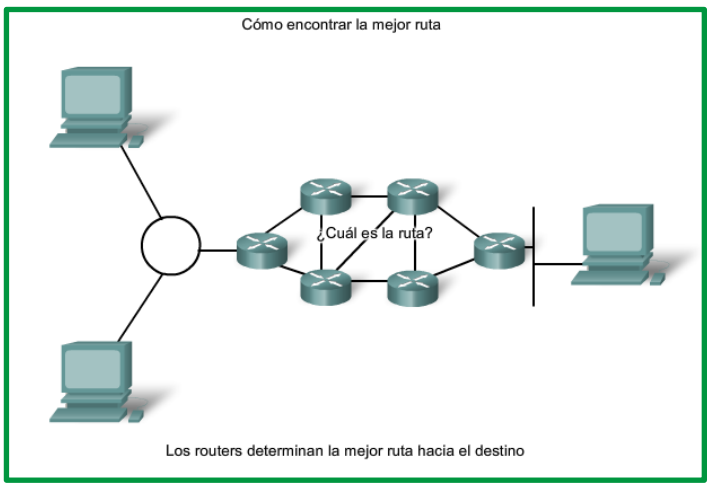


Figure 31. Como determinar la mejor ruta

Función de conmutación

Después de que el router ha determinado la interfaz de salida utilizando la función de determinación de ruta, el router debe encapsular el paquete en la trama de enlace de datos de la interfaz de salida.

La función de conmutación es el proceso utilizado por un router para aceptar un paquete en una interfaz y enviarlo desde otra interfaz. Una responsabilidad clave de la función de conmutación es la de encapsular los paquetes en el tipo de trama de enlace de datos correcto para el enlace de datos de salida.

¿Qué hace un router cuando recibe un paquete desde una red y está destinado a otra red? El router ejecuta los tres siguientes pasos principales:

1. Desencapsula el paquete de Capa 3 al quitar el tráiler y el encabezado de trama de Capa 2.

2. Examina la dirección IP de destino del paquete IP para encontrar la mejor ruta en la tabla de enrutamiento.

3. Encapsula el paquete de Capa 3 en una nueva trama de Capa 2 y envía la trama desde la interfaz de salida.

Ejemplo:

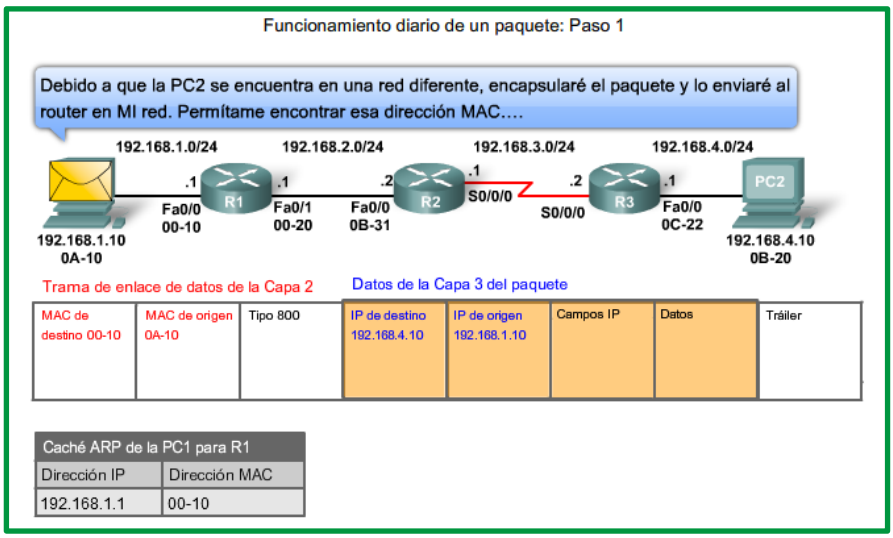


Figure 32. Proceso de envio de paquete capa 3 - Paso 1

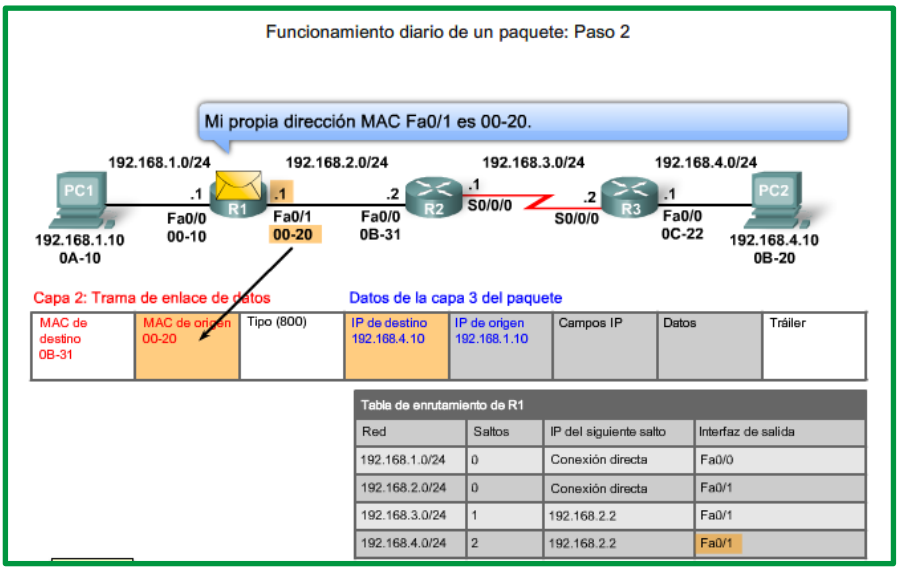


Figure 33. Proceso de envio de paquete capa 3 - Paso 2

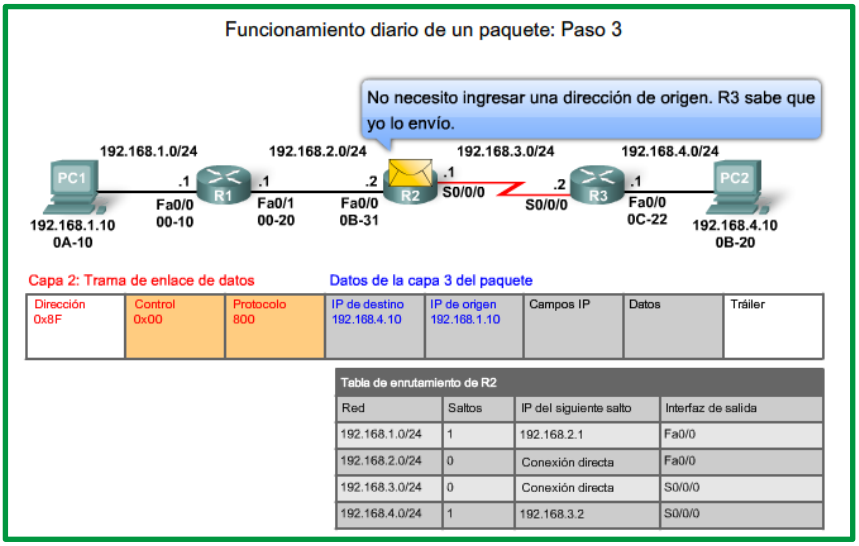


Figure 34. Proceso de envio de paquete capa 3 - Paso 3

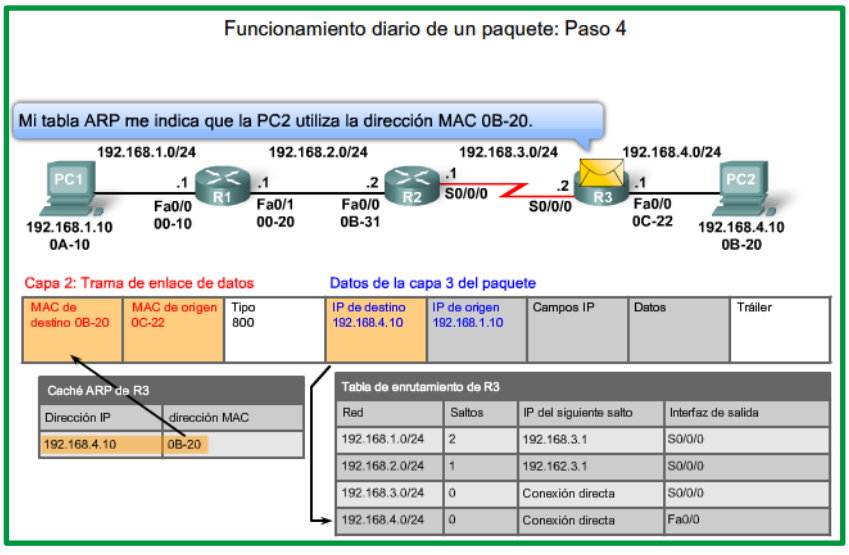


Figure 35. Proceso de envió de paquete capa 3 - Paso 4

Enrutamiento estático

Las rutas a redes remotas con los siguientes saltos asociados se pueden configurar manualmente en el router. Esto se conoce como enrutamiento estático. Una ruta default también puede ser configurada estáticamente.

Si el router está conectado a otros routers, se requiere conocimiento de la estructura de internetworking. Para asegurarse de que los paquetes están enrutados para utilizar los mejores posibles siguientes saltos, cada red de destino necesita tener una ruta o una ruta default configurada. Como los paquetes son reenviados en cada salto, cada router debe estar configurado con rutas estáticas hacia los siguientes saltos que reflejan su ubicación en la internetwork.

Además, si la estructura de internetwork cambia o si se dispone de nuevas redes, estos cambios tienen que actualizarse manualmente en cada router. Si no se realiza la actualización periódica, la información de enrutamiento puede ser incompleta e inadecuada, causando demoras y posibles pérdidas de paquetes.

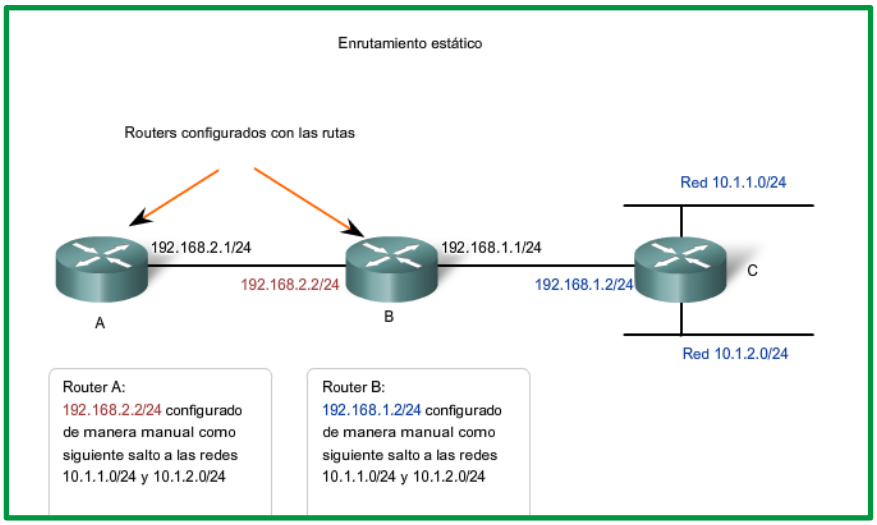


Figure 36. Rutas estáticas

Enrutamiento dinámico

Aunque es esencial que todos los routers en una internetwork posean conocimiento actualizado, no siempre es factible mantener la tabla de enrutamiento por configuración estática manual. Por eso, se utilizan los protocolos de enrutamiento dinámico. Los protocolos de enrutamiento son un conjunto de reglas por las que los routers comparten dinámicamente su información de enrutamiento. Como los routers advierten los cambios en las redes para las que actúan como gateway, o los cambios en enlaces entre routers, esta información pasa a otros routers. Cuando un router recibe información sobre rutas nuevas o modificadas, actualiza su propia tabla de enrutamiento y, a su vez, pasa la información a otros routers. De esta manera, todos los routers cuentan con tablas de enrutamiento actualizadas dinámicamente y pueden aprender sobre las rutas a redes remotas en las que se necesitan muchos saltos para llegar. La figura muestra un ejemplo de rutas que comparten un router.

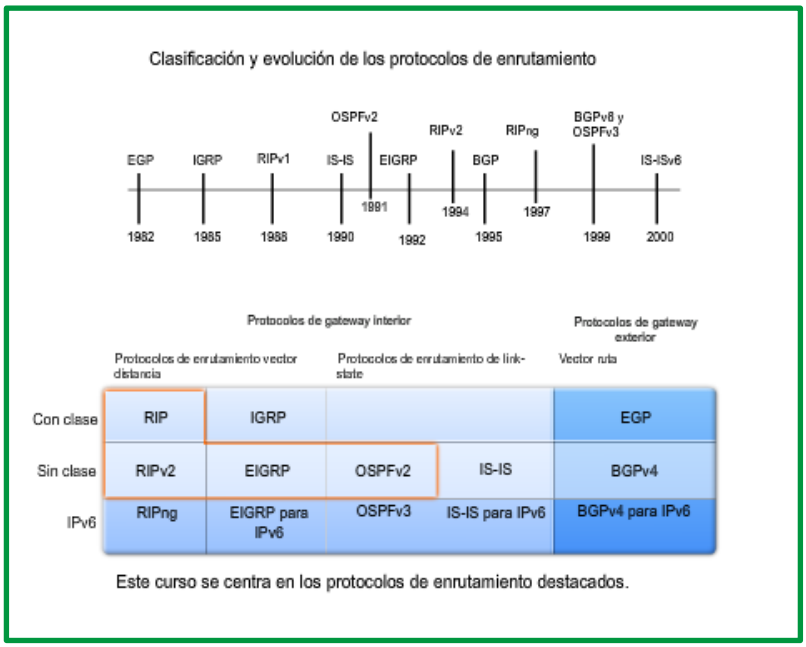


Figure 37. Clasificación y evolución de los protocolos de enrutamiento

Entre los protocolos de enrutamiento comunes se incluyen:

- protocolo de información de enrutamiento (RIP),
- protocolo de enrutamiento de gateway interior mejorado (EIGRP), y
- Open Shortest Path First (OSPF).

Aunque los protocolos de enrutamiento proveen routers con tablas de enrutamiento actualizadas, existen costos. Primero, el intercambio de la información de la ruta agrega una sobrecarga que consume el ancho de banda de la red. Esta sobrecarga puede ser un problema, particularmente para los enlaces del ancho de banda entre routers. Segundo, la información de la ruta que recibe un router es procesada extensamente por protocolos como EIGRP y OSPF para hacer las entradas a las tablas de enrutamiento. Esto significa que los routers que emplean estos protocolos deben tener suficiente capacidad de procesamiento como para implementar los algoritmos del protocolo para realizar el enrutamiento oportuno del paquete y enviarlo.

El enrutamiento estático no produce sobrecarga de la red ni ubica entradas dinámicamente en la tabla de enrutamiento; el router no necesita ningún tipo de procesamiento. El costo para un enrutamiento estático es administrativo, la configuración manual y el mantenimiento de la tabla de enrutamiento aseguran un enrutamiento eficiente y efectivo.

En muchas internetworks, la combinación de rutas estáticas, dinámicas y default se usa para proveer las rutas necesarias.

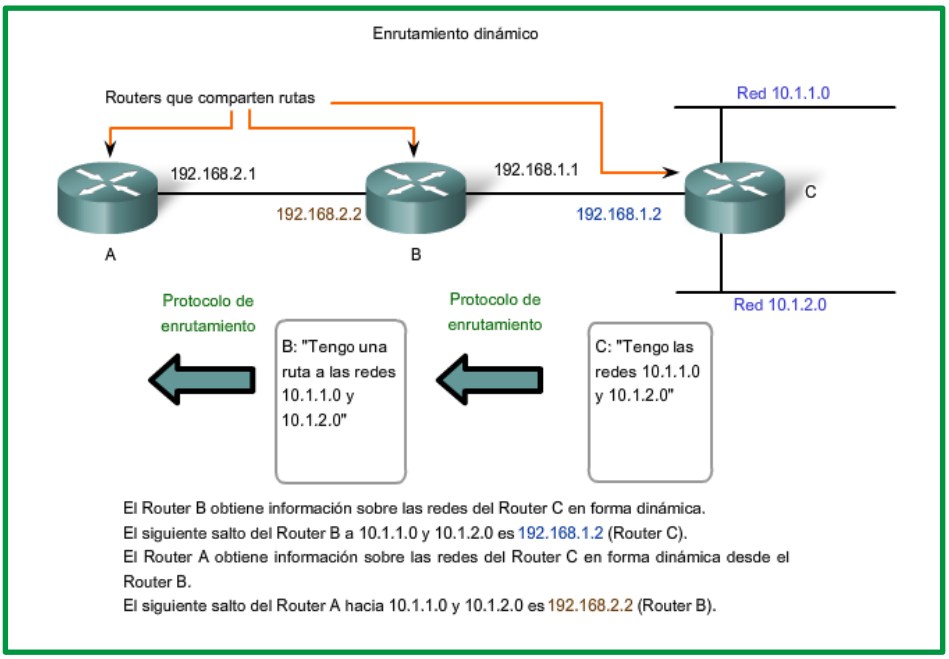


Figure 38. Aplicación de enrutamiento Dinámico

Uno de punto importante de este estudio es mostrar los diferentes algoritmos de enrutamiento que resuelven esta cuestión, y a su vez compararlos en forma cualitativa para conocer cuáles son sus fortalezas y cuáles son sus puntos débiles.

El objetivo principal del protocolo de enrutamiento es determinar las mejores trayectorias para cada ruta a fin de incluirlas en la tabla de enrutamiento. El algoritmo de enrutamiento genera un valor, o una métrica, para cada ruta a través de la red. Las métricas se pueden calcular sobre la base de una sola característica o de varias características de una ruta. Algunos protocolos de enrutamiento pueden basar la elección de la ruta en varias métricas, combinándolas en un único valor métrico. Cuanto menor es el valor de la métrica, mejor es la ruta.

Los protocolos de enrutamiento se agrupan en Protocolos de gateway interiores(IGP) y Protocolos de gateway exterior (EGP).

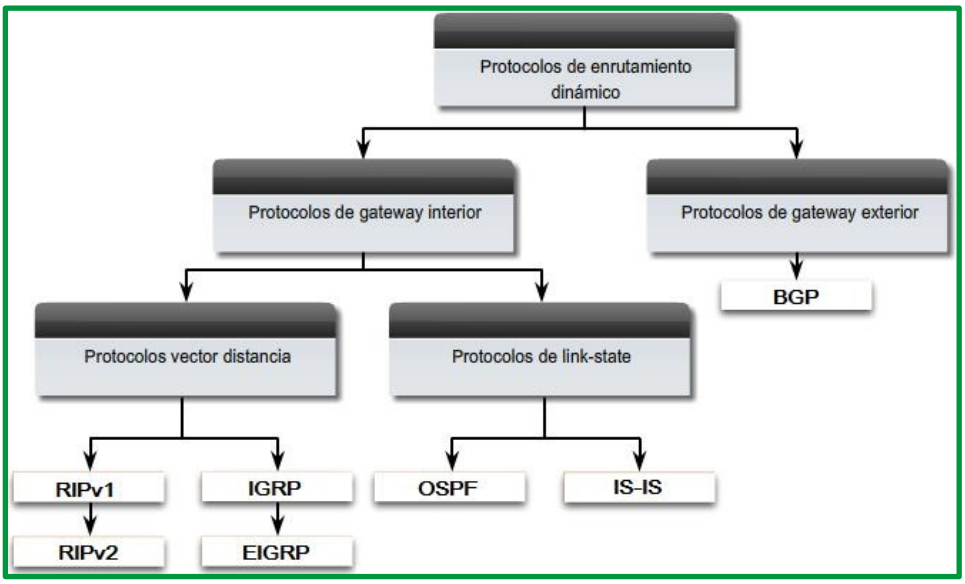


Figure 39. Protocolos de enrutamiento

La tabla a continuación clasifica los protocolos de enrutamiento. Los ***Interior Gateway Protocols*** (IGPs) son protocolos de enrutamiento utilizados para intercambiar información de enrutamiento dentro de un dominio de enrutamiento administrado por una sola organización. Sólo hay un EGP y es BGP. BGP se utiliza para intercambiar información de enrutamiento entre diferentes organizaciones, conocidos como sistemas autónomos (AS). Los ISP utilizan BGP para enrutar paquetes a través de Internet. Los protocolos de enrutamiento vectorial de distancia, estado de vínculo y vector de ruta se refieren al tipo de algoritmo de enrutamiento utilizado para determinar la mejor ruta.

Tabla 3. Protocolos de enrutamientos

	Interior Gateway Protocols				Exterior Gateway Protocols
	Vector distancia		**Estado de enlace**		**Vector ruta**
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP para IPv6	OSPFv3	IS-IS para IPv6	BGP-MP

Convergencia.

La convergencia es el objetivo principal de todos los protocolos de enrutamiento. Cuando un conjunto de enrutadores converge significa que todos sus elementos se han puesto de acuerdo y reflejan la situación real del entorno de red donde se encuentran. La velocidad con la que los protocolos convergen después de un cambio es una buena medida de la eficacia del protocolo de enrutamiento.

Interconexión de redes

Uno de los desafíos en las arquitecturas de redes es la interconexión del conjunto de redes de existente independiente de su naturaleza.

Las subredes que forman parte de interred son heterogenias que requieren ser interconectadas entre sí para formar parte de la red global que le permita la comunicación de los dispositivos

conectados a cualquiera de la subred. En todos los casos, los protocolos de red definen las características de la conexión.

El fin primordial de conectar equipos a una red adquiere otra dimensión cuando la complejidad de las redes a los que los usuarios se conectan aumenta. Se pretende que dialoguen usuarios que están conectados a redes de distintas tecnologías (p.ej.: Ethernet, Token Ring, FDDI, X.25, Frame Relay, ATM...). Sin embargo, nos encontramos con múltiples dificultades:

- Pueden estar soportadas por medios físicos diferentes, ya sean cableados (por ejemplo, fibra óptica, par trenzado, coaxial fino o grueso, etc.) o inalámbricos (por ejemplo, WLAN, enlaces satelitales, etc.).
- Pueden soportar diferentes velocidades (por ejemplo, FDDI a 100 Mbps, Ethernet a 10, 100 Mbps o 1 Gbps).
- Con respecto al tamaño máximo de transmisión, cada red puede permitir una MTU (Maximum Transmition Unit) diferente.
- Unas subredes pueden ser orientadas a conexión y otras no.
- En unos casos el servicio que ofrezcan será fiable (X.25) y en otros no (Ethernet).
- El enrutamiento, cada red puede aplicar diferentes técnicas (estáticas o dinámicas, centralizadas o distribuidas).

Todo lo anterior supone un problema a la hora de ofrecer una comunicación a los dispositivos conectados a la red global (a la interred) extremo a extremo. El fin último de la interred será que se comuniquen dispositivos conectados a las diferentes subredes de distintas tecnologías (por ejemplo, Ethernet, Token-Ring, FDDI, X.25, Frame-Relay o ATM) que la forman. Para ello se deberán superar todas las dificultades anteriores.

La solución más simple de conectar las diferentes subredes consiste en utilizar los denominados ***Sistemas Intermedios*** o de Interconexión (SI) que constituyen una especie de pasarela entre las subredes de diferente (o igual) tecnología. En la figura siguiente se presenta una interred formada por 4 subredes de diferente naturaleza (ATM, Frame-Relay, Token-Ring y Ethernet), interconectadas entre sí mediante cinco SI. En ella aparecen dos sistemas finales o SF (uno conectado a la subred ATM y otro a la subred Ethernet) que son los dispositivos que desean comunicarse.

Los sistemas intermedios, también denominados Internetworking Units (IWU), son sistemas auxiliares que interconectan subredes y que no incluirán necesariamente todos los niveles de la arquitectura OSI (Open System Interconnection). Normal-mente incluirán, como máximo, hasta la capa 3, aunque pueden incluir capas superiores o funcionalidades de las mismas. Pueden ser desde simples conectores o adaptadores de medios hasta encaminadores o routers muy complejos. (Fernando Boronat Seguí, 2013)

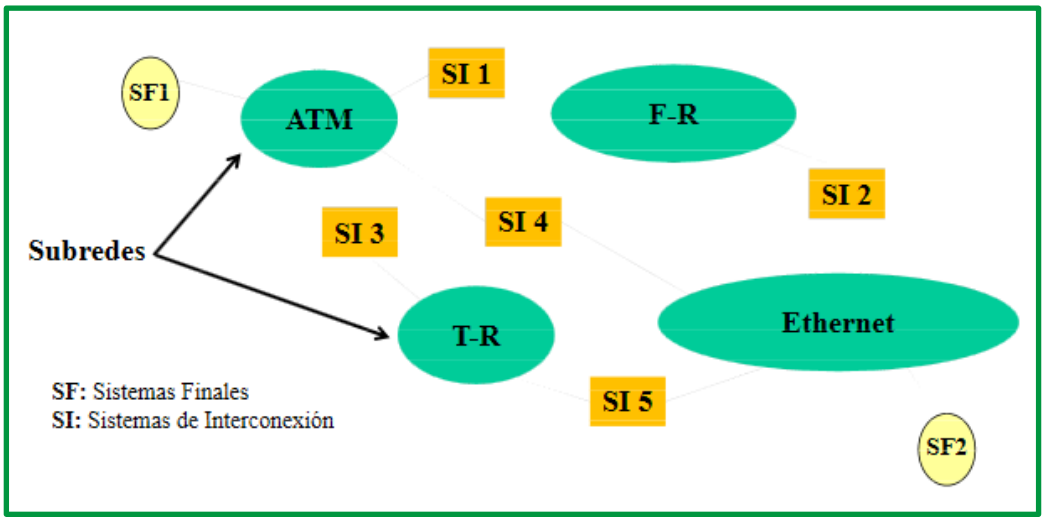


Figure 40. Interconexión de subredes mediante sistemas intermedios

La idea del modelo OSI es que sólo se pueda establecer un diálogo directo entre niveles homólogos de las diferentes capas del modelo, es decir, entre los mismos niveles (que hablan el mismo 'idioma' o protocolo de comunicaciones). Cuando no lo son, se necesitará un sistema intermedio (SI) para la conversión de un protocolo a otro.

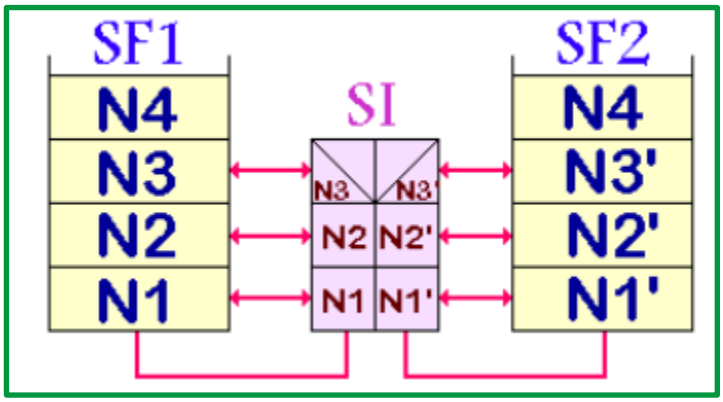


Figure 41. Interconexión de subredes mediante sistemas intermedios

Para interconectar redes entre sí o bien segmentos de red se emplean una serie de dispositivos de interconexión, como son los repetidores, puentes, encaminadores (routers), pasarelas (gateways) y los hubs o dispositivos de concentración.

Los ***repetidores*** realizan la interconexión a nivel físico. Su función consiste en amplificar y regenerar la señal, compensando la atenuación y distorsión debidas a la propagación por el medio físico. Son, por consiguiente, transparentes al subnivel MAC y superiores. Las características más significativas de los repetidores son:

- ✓ Permiten incrementar la longitud de la red.
- ✓ Operan con cualquier tipo de protocolo, ya que sólo trabajan con señales físicas.
- ✓ No procesan tramas, con lo que el retardo es mínimo.
- ✓ Son de bajo coste, debido a su simplicidad.

- ✓ El número total de repetidores que se pueden incorporar en una red está limitado por la longitud máxima de la misma debido a la arquitectura, por ejemplo, 2500 m en IEEE 802.3 ó Ethernet.
- ✓ No aíslan tráfico, es decir, el ancho de banda del medio está compartido por todas las estaciones, independientemente de la sección de la red en que estén ubicadas.
- ✓ Se utilizan tanto redes de área local como en redes de área extensa.

Los ***puentes*** son elementos que operan a nivel de enlace. En consecuencia, lógica es más compleja que la de los repetidores, siendo naturalmente más costoso. Sus características más significativas son:

- ✓ Permiten aislar tráfico entre segmentos de red
- ✓ Operan transparentemente al nivel de red y superiores
- ✓ No hay limitación conceptual para el número de puentes en una red.
- ✓ Procesan las tramas, lo que aumenta el retardo.
- ✓ Utilizan algoritmos de encaminamiento, que generan tráfico adicional en la red.
- ✓ Filtran las tramas por dirección física y por protocolo.
- ✓ Se utilizan en redes de área local.

Los ***encaminadores*** realizan transformaciones a nivel de red. En consecuencia, todos los nodos de la red deben tener un nivel de red determinado. Son transparentes a los niveles superiores al nivel de red. Sus características más significativas son:

- ✓ Permiten aislar totalmente segmentos de red, con lo que éstos pasan a ser redes independientes o subredes.
- ✓ Permiten interconectar cualquier tipo de red: Paso de testigo. Ethernet, X.25, etc.
- ✓ No hay limitación conceptual para el número de encaminadores en una red.
- ✓ Requieren la utilización de un nivel de red determinado.
- ✓ El proceso en los encaminadores es más complejo que en los puentes, por lo que el retardo es mayor.
- ✓ Son los elementos más complejos y, en consecuencia, más costosos.
- ✓ Se utilizan tanto en redes de área local como de área extensa

Las ***pasarelas*** realizan transformaciones a niveles superiores al nivel de red. Se utilizan para interconectar aplicaciones, equipos, sistemas o redes de distintas arquitecturas, por ejemplo, para transformar correo X.400 en correo TEC/IP.

Los ***hubs***, expresión de difícil traducción en este contexto, originalmente realizaban concentración de cableado. Los primeros hubs eran concentradores/repetidores que permitían la conexión de un número determinado de dispositivos a la red principal.

Posteriormente aparecieron los hubs multimedia, que permitían la conexión a diversos medios físicos. Por último, aparecen los hubs de tercera generación, que, mediante la incorporación de puentes, encaminadores o conmutadores, permiten la interconexión de redes de distinto protocolo, incorporando además posibilidades de gestión de red.

Con lo antepuesto se pude determinar que existe Interconexión a:

✓ **Nivel Físico**: Un sistema de interconexión de nivel 1 (nivel físico) será necesario cuando se desee conectar dos subredes con todos los niveles iguales salvo el nivel físico. El SI realizará funciones de pasarela entre, al menos, ambos niveles físicos, tal y como se muestra en la figura.

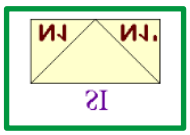


Figure 42. Interconexión a nivel físico

Existen dos tipos de sistemas de interconexión de nivel físico: los activos y los pasivos. Por un lado, tenemos los denominados ***adaptadores de impedancias***, que son dispositivos pasivos. Por otro lado, tenemos los ***repetidores*** que son activos ya que regeneran, amplifican la señal y, si es necesario, convierten formatos.

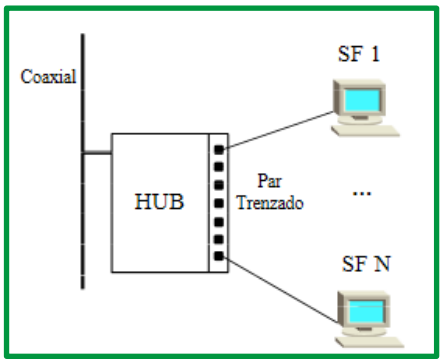


Figure 43. Conexión mediante un hub con puertos de par trenzado y puertos coaxiales

✓ **Nivel de enlace de datos**: En este caso es el nivel 2 el que diferencia ambas subredes (si además el 1 es diferente usaríamos esto mismo).

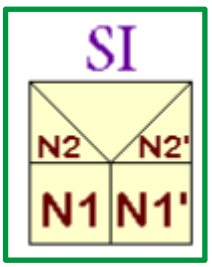


Figure 44. Interconexión a nivel de enlace.

Estos sistemas intermedios (denominados bridges o puentes) deben ser inteligentes (CPU + memoria), pues deben entender y procesar las tramas de nivel 2.

Podemos simplificar su funcionamiento:

1. El bridge se dedica a escuchar las tramas del Token Ring(TR) y de Ethernet.
2. Cada trama que llega se copia en su memoria interna.
3. La CPU analiza C2 (cabecera de nivel 2 del TR en este caso). Si el destino está en el TR descarta la trama, pues se supone que de A a B llegará sin problemas.

4. Si el destino está en la red Ethernet, crea una cabecera C2' (cabecera Ethernet de nivel 2) convirtiendo C2 y rellena el campo de datos con los datos originales (los de C2).

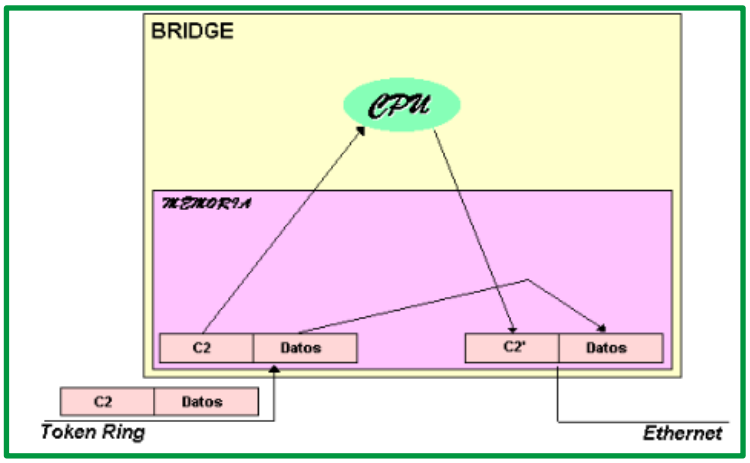


Figure 45. Funcionamiento de un bridge.

✓ **Nivel de red**: Es el caso en el que los equipos implicados se encuentran situados en dominios o "subredes" que, aunque comparten niveles superiores, difieren en mayor o menor medida en los tres niveles básicos del modelo de referencia correspondiente.

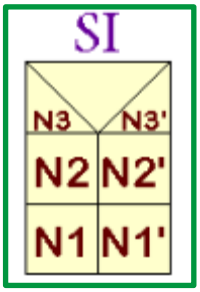


Figure 46. Interconexión a nivel de red.

Los sistemas intermedios encargados de realizar esta función se llaman routers, encaminadores o enrutadores.

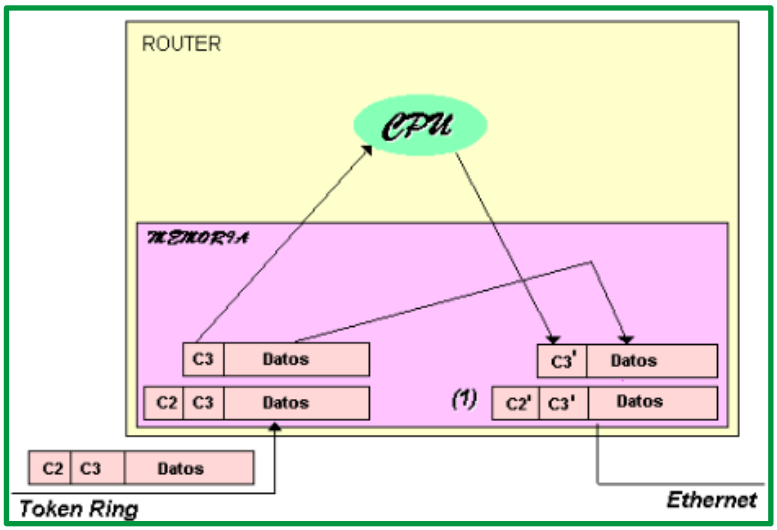


Figure 47. Funcionamiento de un router.

El modo de funcionamiento en este caso sería:

1. Después de copiar en memoria la trama de nivel 2, corta y tira su cabecera. 2.
2. Del campo de datos saca la trama de nivel 3 y analiza su cabecera (C3) en la CPU. 3.En base a C3:
   - ✓ Encaminará.
   - ✓ Generará C3’ y en definitiva otra PDU de nivel 3 (con los mismos datos que tenía la de C3).
   - ✓ Generará tramas de nivel 2 con C2' (la dirección origen de C2' será el punto (1) de la figura y no la del TR como ocurría en el caso anterior).

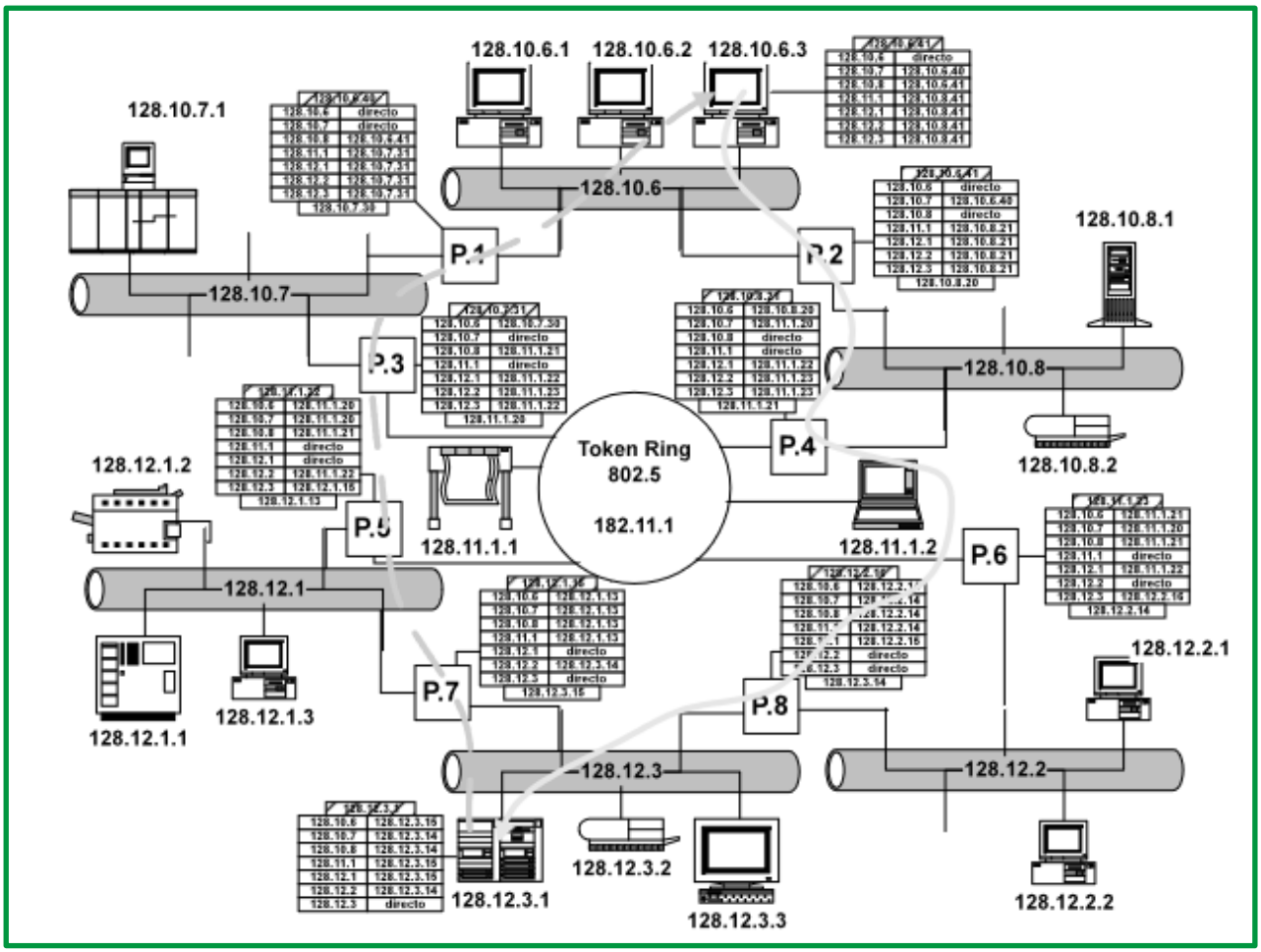


Figure 48. Ejemplo de red con las tablas de los encaminadores.

- ✓ **Nivel de interred**: Existen casos en los que no es posible la conversión directa de los diferentes niveles de Red, o que simplemente, no existe un método concreto para llevar a cabo la conversión. Como solución, se plantea la posibilidad de buscar una solución intermedia común a ambos extremos. Para ello, se añadirá un nuevo nivel (Nivel de Interred) que estará en todos los sistemas y que evitará la conversión de un protocolo a otro.

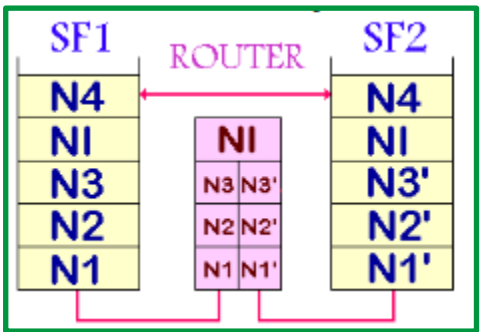


Figure 49. Nivel de interred.

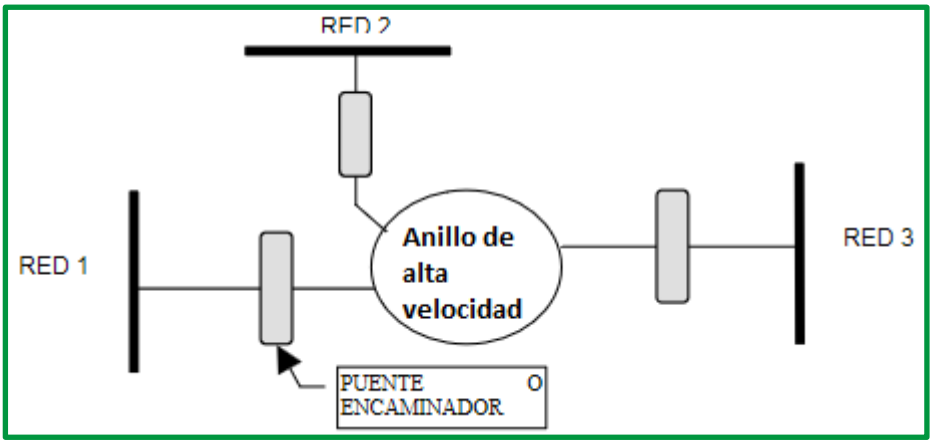


Figure 50. Interconexión de redes mediante anillo de alta velocidad.

La encapsulación de unos protocolos dentro de otros es la solución más ampliamente difundida para resolver el problema de circulación de información en redes heterogéneas. De esta manera se solventa, por ejemplo, el problema de la transmisión de información de una red SNA a través de una red TCP/IP para llegar como destino a otra red SNA (véase la figura siguiente).

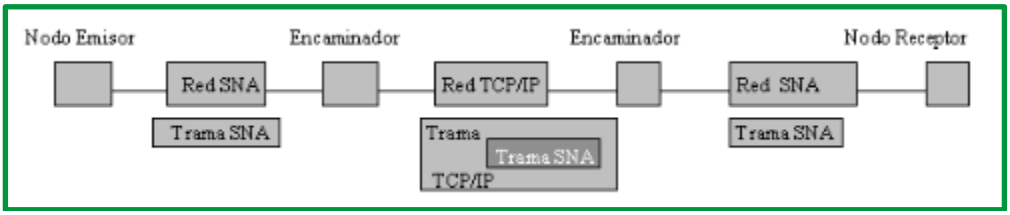


Figure 51. Ejemplo de red en la que tanto el emisor como el receptor de los mensajes están conectados a redes SNA y sin embargo, la información debe circular atravesando una red TCP/IP.

En la siguiente figura se puede observar un ejemplo de aplicación de pasarela:

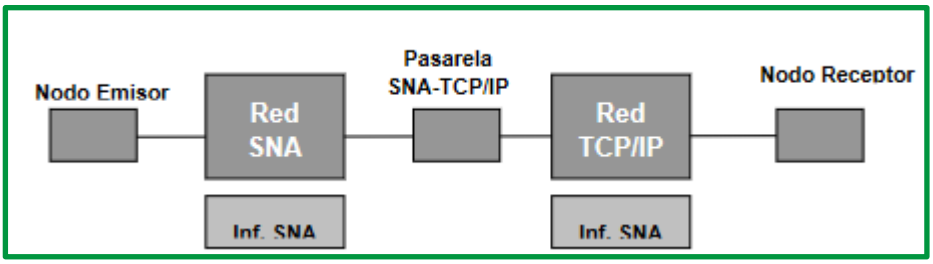


Figure 52. Empleo de pasarela SNA-TCP/IP para la transformación de información de protocolo entre ambas arquitecturas.

Capa de red de internet

La cual corresponde con el nivel de red o capa de red, según la normalización OSI. Es un nivel o capa que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Su misión es conseguir que los datos lleguen desde el origen al destino, aunque no tengan conexión directa. Ofrece servicios al nivel superior (nivel de transporte) y se apoya en el nivel de enlace.

La Capa de red o Capa 3 de OSI provee servicios para intercambiar secciones de datos individuales a través de la red entre dispositivos finales identificados. Para realizar este transporte de extremo a extremo la Capa 3 utiliza cuatro procesos básicos:

Direccionamiento: ***Primero***, la Capa de red debe proveer un mecanismo para direccionar estos dispositivos finales. Si las secciones individuales de datos deben dirigirse a un dispositivo final, este dispositivo debe tener una dirección única. En una red IPv4, cuando se agrega esta dirección a un dispositivo, al dispositivo se lo denomina host.

Encapsulamiento: ***Segundo***, la capa de Red debe proveer encapsulación. Los dispositivos no deben ser identificados sólo con una dirección; las secciones individuales, las PDU de la capa de Red, deben, además, contener estas direcciones. Durante el proceso de encapsulación, la Capa 3 recibe la PDU de la Capa 4 y agrega un encabezado o etiqueta de Capa 3 para crear la PDU de la Capa 3. Cuando nos referimos a la capa de Red, denominamos paquete a esta PDU. Cuando se crea un paquete, el encabezado debe contener, entre otra información, la dirección del host hacia el cual se lo está enviando. A esta dirección se la conoce como dirección de destino. El encabezado de la Capa 3 también contiene la dirección del host de origen. A esta dirección se la llama dirección de origen. Después de que la Capa de red completa el proceso de encapsulación, el paquete es enviado a la capa de enlace de datos que ha de prepararse para el transporte a través de los medios.

Enrutamiento: Luego, la capa de red debe proveer los servicios para dirigir estos paquetes a su host destino. Los hosts de origen y destino no siempre están conectados a la misma red. En realidad, el paquete podría recorrer muchas redes diferentes. A lo largo de la ruta, cada paquete debe ser guiado a través de la red para que llegue a su destino final. Los dispositivos intermediarios que conectan las redes son los routers. La función del router es seleccionar las rutas y dirigir paquetes hacia su destino. A este proceso se lo conoce como enrutamiento.

Desencapsulamiento: Finalmente, el paquete llega al host destino y es procesado en la Capa 3. El host examina la dirección de destino para verificar que el paquete fue direccionado a ese dispositivo. Si la dirección es correcta, el paquete es desencapsulado por la capa de Red y la PDU de la Capa 4 contenida en el paquete pasa hasta el servicio adecuado en la capa de Transporte.

Los protocolos implementados en la capa de Red que llevan datos del usuario son:

- Versión 4 del Protocolo de Internet (IPv4)
- Versión 6 del Protocolo de Internet (IPv6)
- Intercambio Novell de paquetes de internetwork (IPX)
- AppleTalk
- Servicio de red sin conexión (CLNS/DECNet)

IPv4

La versión 4 de IP (IPv4) es la versión de IP más ampliamente utilizada. Es el protocolo de Capa 3 que se utiliza para llevar datos de usuario a través de Internet.

El ***protocolo IP*** es parte de la capa de Internet del conjunto de protocolos TCP/IP. Es uno de los protocolos de Internet más importantes ya que permite el desarrollo y transporte de datagramas de IP (paquetes de datos), aunque sin garantizar su "entrega". En realidad, el protocolo IP procesa datagramas de IP de manera independiente al definir su representación, ruta y envío.

El protocolo de Internet fue diseñado como un protocolo con bajo costo. Provee sólo las funciones necesarias para enviar un paquete desde un origen a un destino a través de un sistema interconectado de redes. El protocolo no fue diseñado para rastrear ni administrar el flujo de paquetes. Estas funciones son realizadas por otros protocolos en otras capas. Características básicas de IPv4:

- **Sin conexión**: No establece conexión antes de enviar los paquetes de datos.

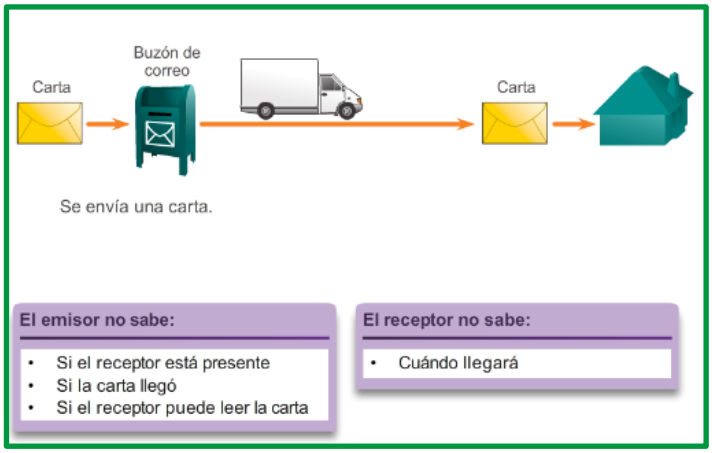


Figure 53. Comunicación sin conexión

- **Máximo esfuerzo** (no confiable): No se usan encabezados para garantizar la entrega de paquetes.

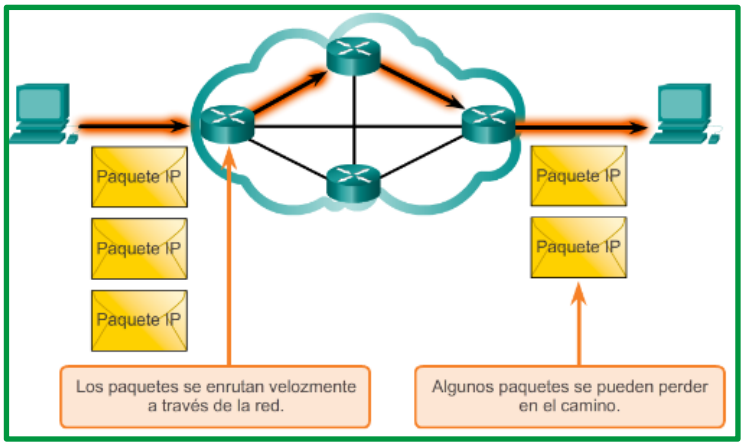


Figure 54. Máximo esfuerzo

- **Medios independientes**: Operan independientemente del medio que lleva los datos.

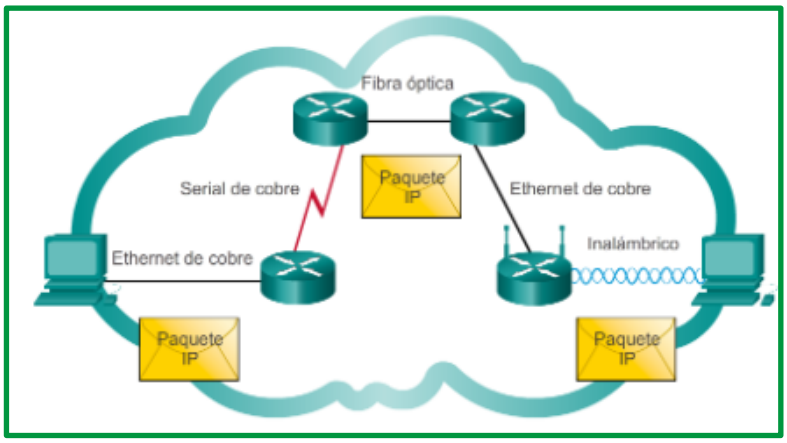


Figure 55. Independencia de los medios

El protocolo IP determina el destinatario del mensaje mediante 3 campos:

- ***El campo de dirección IP***: Dirección del equipo.
- ***El campo de máscara de subred***: Una máscara de subred le permite al protocolo IP establecer la parte de la dirección IP que se relaciona con la red.
- ***El campo de pasarela predeterminada***: Le permite al protocolo de Internet saber a qué equipo enviar un datagrama, si el equipo de destino no se encuentra en la red de área local.

Formato de paquete de Internet Protocol (IP)

El ***Internet Protocol*** especificado en RFC 791 define el formato de paquete IP. El encabezado del paquete IP tiene campos específicos que contienen información sobre el paquete y sobre los host emisores y receptores. La siguiente es una lista de los campos en el encabezado IP y una breve descripción de cada uno. Ya debe conocer de cerca los campos de dirección IP de destino, dirección IP de origen, versión y Período de vida (TTL).

- ***Versión***: Número de versión (4 bits); la versión predominante es la IP versión 4 (IPv4)
- ***Longitud del encabezado IP***: También denominado *IHL* por *Internet Header Length (Longitud del encabezado de Internet)* longitud del encabezado en palabras de 32 bits (4 bits)
- ***Prioridad y tipo de servicio***: Cómo debe administrarse el datagrama (8 bits); los primeros 3 bits son bits de prioridad (este uso ha sido reemplazado por el Punto de código de servicios diferenciados [Differentiated Services Code Point, DSCP], que usa los primeros 6 bits [se reservan los últimos 2])
- ***Longitud del paquete***: Longitud total (encabezado + datos) (16 bits); indica el tamaño total del datagrama en bytes. El tamaño de este campo es de 2 bytes, por lo tanto, el tamaño total del datagrama no puede exceder los 65536 bytes. Si se lo utiliza junto con el tamaño del encabezado, este campo permite determinar dónde se encuentran los datos.
- ***Identificación***: Valor único del datagrama IP (16 bits), son campos que permiten la fragmentación de datagramas.
- ***Señalizadores***: Controlan la fragmentación (3 bits)

- ***Desplazamiento de fragmentos***: Admite la fragmentación de datagramas para permitir diferentes unidades máximas de transmisión (MTU) en Internet (13 bits)
- ***Período de vida (TTL)***: Identifica cuántos routers puede atravesar el datagrama antes de ser descartado (8 bits), por lo tanto, este campo disminuye con cada paso por un router y cuando alcanza el valor crítico de 0, el router destruye el datagrama. Esto evita que la red se sobrecargue de datagramas perdidos.
- ***Protocolo***: Protocolo de capa superior que envía el datagrama (8 bits), este campo, en notación decimal, permite saber de qué protocolo proviene el datagrama: ICMP: 1, IGMP: 2, TCP: 6, UDP: 17.
- ***Checksum del encabezado***: Este campo contiene un valor codificado en 16 bits que permite controlar la integridad del encabezado para establecer si se ha modificado durante la transmisión. La suma de comprobación es la suma de todas las palabras de 16 bits del encabezado (se excluye el campo suma de comprobación). Esto se realiza de tal modo que cuando se suman los campos de encabezado (suma de comprobación inclusive), se obtenga un número con todos los bits en 1.
- ***Dirección IP de origen***: Dirección IP de origen de 32 bits (32 bits)
- ***Dirección IP de destino***: Dirección IP de destino de 32 bits (32 bits)
- ***Opciones de IP***: Pruebas de red, depuración, seguridad y otras (0 ó 32 bits, si corresponde)

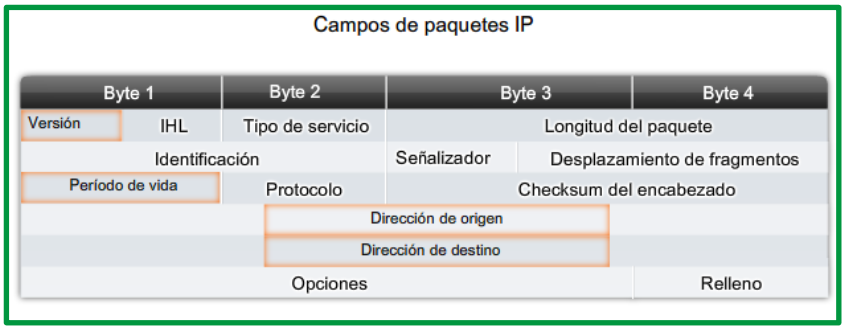


Figure 56. Campos de Paquetes IP

IPv6

El Protocolo de Internet versión 6, en inglés: Internet Protocol version 6 (IPv6), es una versión del Internet Protocol (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet Protocol version 4 (IPv4) RFC 791, que se está implementado en la gran mayoría de dispositivos que acceden a Internet.

IPv6 es una extensión conservadora de IPv4. La mayoría de los protocolos de transporte y aplicación necesitan pocos o ningún cambio para operar sobre IPv6; las excepciones son los protocolos de aplicación que integran direcciones de capa de red, como FTP o NTP.

IPv6 especifica un nuevo formato de paquete, diseñado para minimizar el procesamiento del encabezado de paquetes. Debido a que las cabeceras de los paquetes IPv4 e IPv6 son significativamente distintas, los dos protocolos no son interoperables. Algunos de los cambios de IPv4 a IPv6 más relevantes son:

- Capacidad extendida de direccionamiento

- Autoconfiguración de direcciones libres de estado (SLAAC)
- Multicast
- Seguridad de Nivel de Red obligatoria
- Procesamiento simplificado en los routers
- Movilidad
- Soporte mejorado para las extensiones y opciones
- Jumbogramas

Las direcciones IPv6 tienen una longitud de 128 bits y se escriben como una cadena de valores hexadecimales.

- El sistema hexadecimal es un sistema de base dieciséis.
- El sistema de numeración de base 16 utiliza los números del 0 al 9 y las letras de la A a la F.
- Se pueden representar cuatro bits (medio byte) con un único valor hexadecimal.
- El formato predefinido una dirección IPv6 es x:x:x:x:x:x:x:x, donde cada "x" consta de cuatro valores hexadecimales.

El formato de escritura de una dirección IPv6 debe tomar en cuenta las siguientes reglas:

Regla 1: omitir las 0 iniciales

La primera regla que permite reducir la notación de direcciones IPv6 es que se puede omitir cualquier 0 (cero) inicial en cualquier sección de 16 bits.

01AB puede representarse como 1AB.

09F0 puede representarse como 9F0.

0A00 puede representarse como A00.

00AB puede representarse como AB.

Regla 2: Omitir los segmentos que contienen solamente ceros

Los dos puntos dobles (::) pueden reemplazar cualquier cadena única y contigua de uno o más segmentos de 16 bits que estén compuestas solo por ceros.

Ejemplo: FE80:0:0:0:2AA:FF:FE9A:4CA3 se puede reducir a FE80::2AA:FF:FE9A:4CA3

Pv6 no utiliza la notación decimal punteada de máscara de subred. La longitud de prefijo indica la porción de red de una dirección IPv6 mediante el siguiente formato:

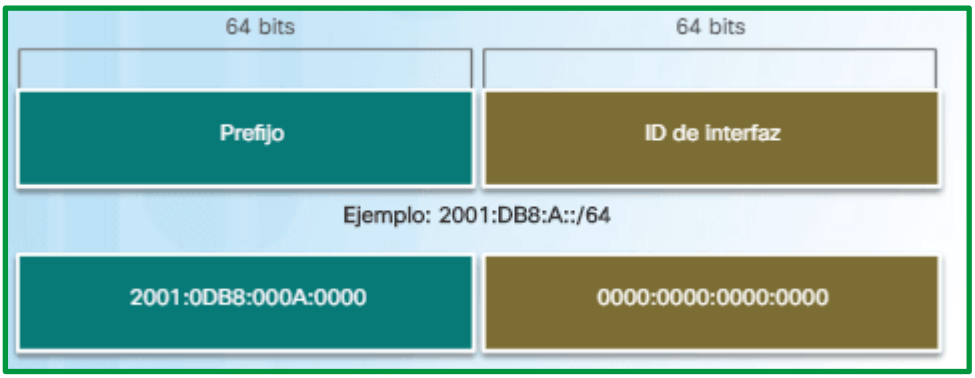


Figure 57. Longitud de prefijo IPv6

- Dirección IPv6 /Longitud de prefijo IPv6
- La longitud de prefijo puede ir de 0 a 128.
- La longitud de prefijo típica es /64.

Existen 3 tipos de direcciones IPv6:

Unicast. Una dirección IPv6 de unidifusión identifica de manera única una interfaz de un dispositivo habilitado para IPv6. Un paquete que se envía a una dirección unicast es recibido por la interfaz que tiene asignada esa dirección, es decir, los paquetes dirigidos a una dirección unicast se envían a una única interfaz. Los tipos de direcciones IPv6 de unidifusión más comunes son las direcciones de unidifusión globales (GUA) y link-local.

Unidifusión globales:

- Similares a direcciones IPv4 públicas.
- Pueden configurarse estáticamente o asignarse de forma dinámica.
- Actualmente, solo se asignan direcciones unicast globales con los tres primeros bits de 001 o 2000::/3 .

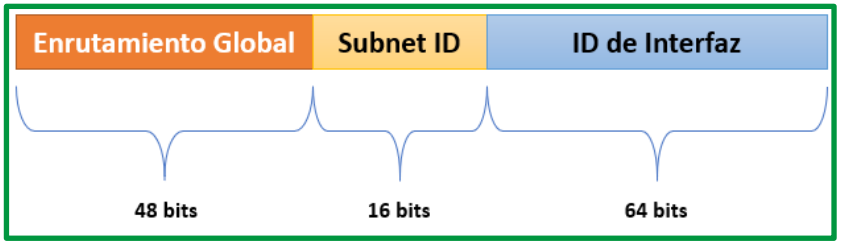


Figure 58. Direcciones IPv6 globales de unicast

***link-local*:**

- Permite que un dispositivo se comunique con otros dispositivos con IPv6 habilitado en el mismo enlace.
- Limitada a un único enlace: no se puede enrutar más allá del enlace.
- Si no se configura manualmente en una interfaz, se creará automáticamente.
- Toda interfaz de red con IPv6 habilitado debe tener una dirección link- local.

- Las direcciones link-local están en el rango de FE80::/10 y se pueden establecer dinámicamente (SLAAC) o como direcciones link-local estáticas. Su analogía a IPv4 es 169.254.0.0./16 .

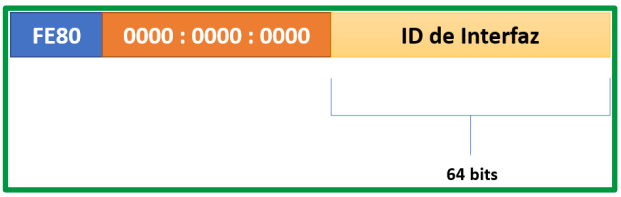


Figure 59. Direcciones IPv6 link local

Loopback:

- Utilizada por los host para enviarse paquetes a sí mismos; no se puede asignar a una interfaz física.
- Hacer ping a la dirección de loopback IPv6 permite probar la configuración de TCP/IP en el host local.
- Formada por todos ceros, excepto el último bit, representado como ::1/128 o, simplemente, ::1.

Dirección sin especificar:

- La dirección formada por todos ceros se representa como ::/128 o simplemente ::
- No puede asignarse a una interfaz y solo se utiliza como dirección de origen.
- Las direcciones sin especificar se utilizan como direcciones de origen cuando el dispositivo aún no tiene una dirección IPv6 permanente o cuando el origen del paquete es irrelevante para el destino.

Direcciones locales unicast:

Se utilizan para el direccionamiento local dentro de un sitio o entre una cantidad limitada de sitios. Estas direcciones no deberían poder enrutarse en la IPv6 global, y no deberían traducirse hacia direcciones IPv6 globales. Las direcciones locales únicas están en el rango de FC00::/7 a FDFF::/7. Es similar a las redes privadas IPv4 (10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/24).

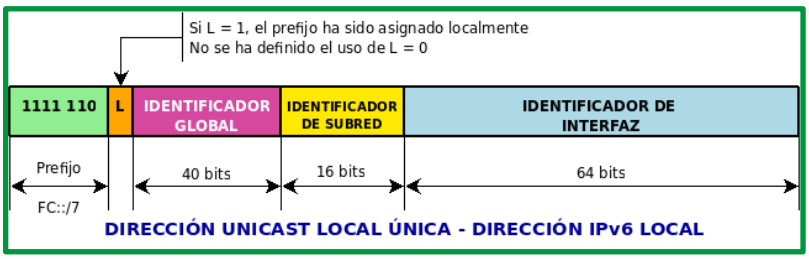


Figure 60. Direcciones IPv6 unique local

- Tiene una estructura de 4 niveles:
  - ✓ Su prefijo es de 7 bits FC00::/7
  - ✓ El bit L puesto a 1 indica que la administración del prefijo es local.
  - ✓ Un indicador global de 40 bits
  - ✓ Un ID de subred de 16 bits de largo
  - ✓ Un ID de interfaz de 64 bits

Se puede realizar agregación de prefijos a nivel de ISP, reduciendo las entradas en las tablas de enrutamiento.

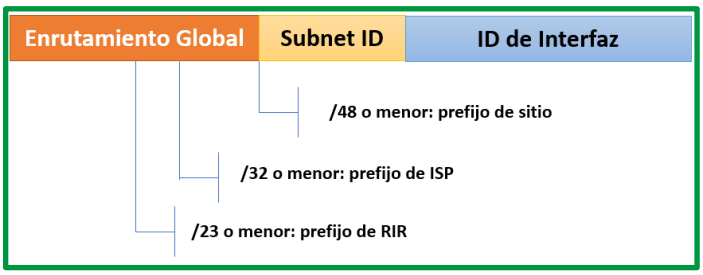


Figure 61. Prefijos a nivel de ISP

Multicast. Las direcciones IPv6 de multidifusión se usan para enviar un único paquete IPv6 a varios destinos y tienen el prefijo FFxx::/8. Dos grupos comunes de direcciones multidifusión IPv6 asignadas incluyen los siguientes:

Grupo multidifusión de todos los nodos FF02::1:

- Se incorporan todos los dispositivos con IPv6 habilitado.
- Tiene el mismo efecto que la dirección IPv4 de broadcast.

Grupo multidifusión de todos los router FF02::2:

- Se incorporan todos los routers IPv6.
- Un router se convierte en un miembro de este grupo cuando se habilita como router IPv6 mediante el comando de configuración global ipv6 unicast-routing.
- Los paquetes que se envían a este grupo son recibidos y procesados por todos los routers IPv6 en el enlace o en la red.

Anycast. Es una dirección para varios dispositivos. Cuando se envía un paquete a una dirección Anycast, se entregará al equipo más cercano que sea propietario de dicha dirección.

Sabías que. - IPv6 no tiene direcciones de broadcast.

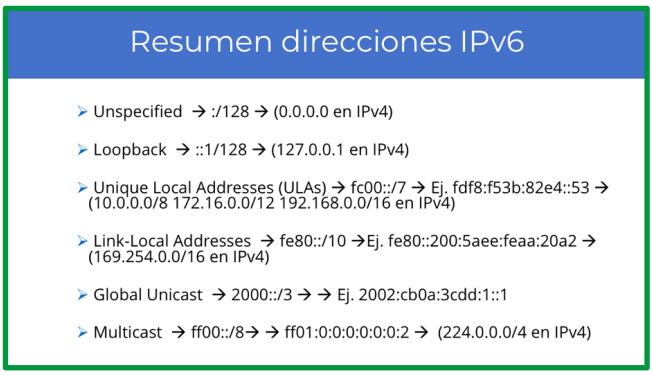


Figure 62. Direcciones IPv6

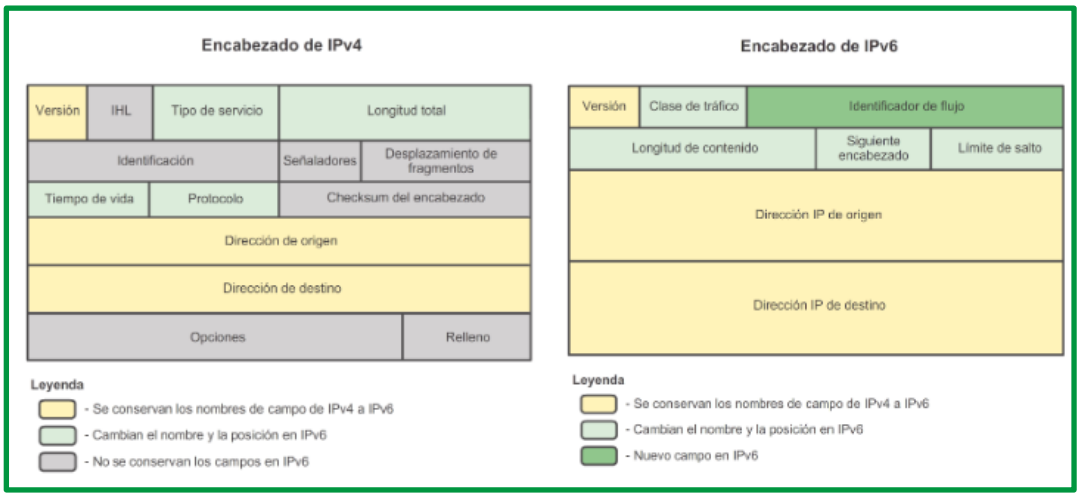


Figure 63. Comparativa encabezado IPv4 e IPv6

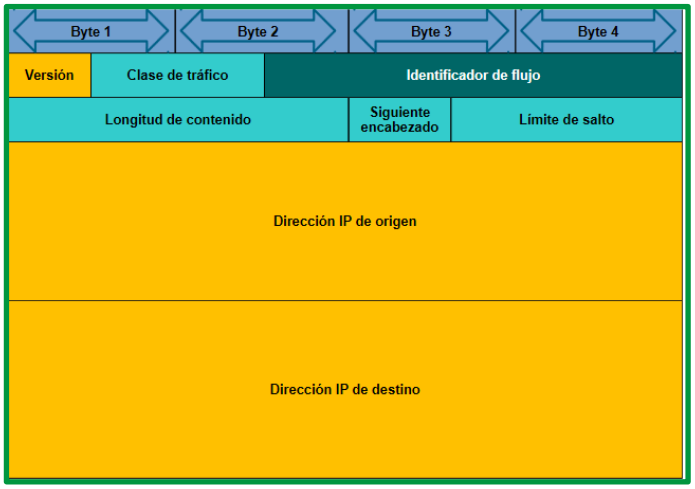


Figure 64. Encabezado IPv6

IPX

IPX. Son las siglas en inglés de Internetwork Packet Exchange (Intercambio de Paquetes Interred). Es un protocolo de la capa de red no orientado a conexión de Netware responsable de transferir datos entre el servidor y los programas de las estaciones de trabajo mediante datagramas.

IPX es un antiguo protocolo de red de Novell perteneciente al sistema operativo NetWare. Se utiliza para transmitir datos a través de la red, incluyendo en cada paquete la dirección de destino. Es un protocolo de datagramas rápido orientado a comunicaciones sin conexión.

Características:

- Se utiliza en un entorno cliente/servidor.
- La dirección es de 80 bits (netwok.node).
- La dirección MAC de interfaz forma parte de la dirección lógica.
- IPX es un protocolo de la Capa de red (nivel 3 del modelo OSI).
- Está orientado a paquetes y a comunicaciones sin conexión (no requiere que se establezca una conexión antes de que los paquetes se envíen a su destino).
- Es utilizado como mensajero del protocolo SPX, ya que por sí solo carece de fiabilidad durante el transporte de paquetes.

- La cabecera de los paquetes de IPX se compone de 30 bytes, y los datos que junto con la cabecera no pueden sobrepasar los 1518 bytes.
- Sistema de direccionamiento IPX.

Se utilizan tres componentes básicos para identificar un proceso en la red:

- ***Dirección de red***, la cual identifica la red a la que pertenece.
- ***Número de nodo*** que indica el dispositivo conectado a la red.
- ***Número de socket*** que indica el proceso en el nodo.

El direccionamiento Novell IPX utiliza una dirección en dos partes: el ***número de red*** y el ***número de nodo***:

> ***El número de red IPX***, asignado por el administrador de red puede tener una longitudad ministrador de red, puede tener una longitud de hasta ocho dígitos hexadecimal.
>
> El ***número de nodo 12 dígitos hexadecimales***, es generalmente la dirección MAC para una interfaz de red en el nodo final. Las interfaces seriales utilizan la dirección MAC de la interfaz Ethernet para su dirección de nodo IPX.

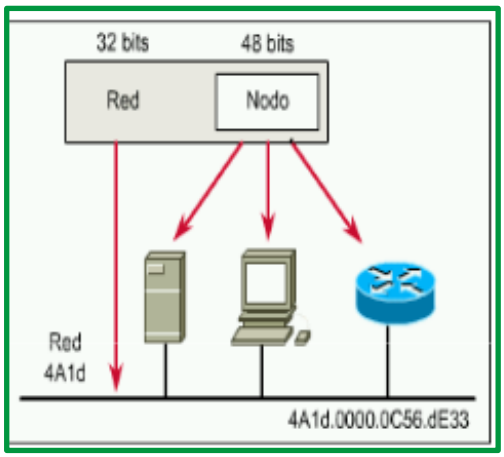


Figure 65. Partes de un direccionamiento Novell IPX

> **RED IPX (*32 bits*).MAC (*48 bits*)**.
>
> El uso de la dirección MAC en la dirección IPX lógica elimina la necesidad de un protocolo de resolución de direcciones (ARP). Novell IPX soporta múltiples redes lógicas en una interfaz individual (subinterfaces); cada red requiere un solo tipo de encapsulamiento.

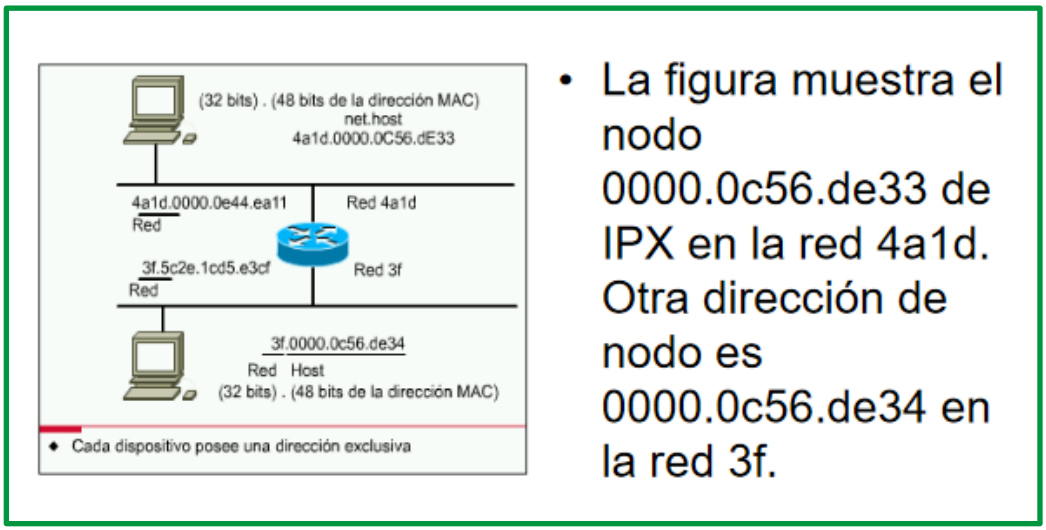


Figure 66. Direccionamiento IPX

El ***protocolo SPX*** (Sequenced Packet eXchange), actúa sobre IPX para asegurar la entrega de los paquetes. Mientras que el protocolo IPX es similar a IP, SPX es similar a TCP. Juntos, por lo tanto, proporcionan servicios de conexión similares a TCP/IP.

AppleTalk

Este protocolo está incluido en el sistema operativo del ordenador Apple Macintosh desde su aparición y permite interconectar ordenadores y periféricos con gran sencillez para el usuario, ya que no requiere ningún tipo de configuración por su parte, el sistema operativo se encarga de todo. Fue incluido en un Macintosh Apple en 1984 y actualmente está en desuso en los Macintosh en favor de las redes TCP/IP, el protocolo utilizado en la capa número 3 es el DDP (Datagram Delivery Protocol) que realiza el transporte de datos de bajo nivel. Existen tres formas básicas de este protocolo:

LocalTalk. Es la forma original del protocolo. La comunicación se realiza por uno de los puertos serie del equipo. La velocidad de transmisión no es muy rápida, pero es adecuada para los servicios que en principio se requerían de ella, principalmente compartir impresoras.

Ethertalk. Es la versión de Appletalk sobre Ethernet. Esto aumenta la velocidad de transmisión y facilita las aplicaciones como la transferencia de ficheros.

Tokentalk. Es la versión de Appletalk para redes Tokenring.

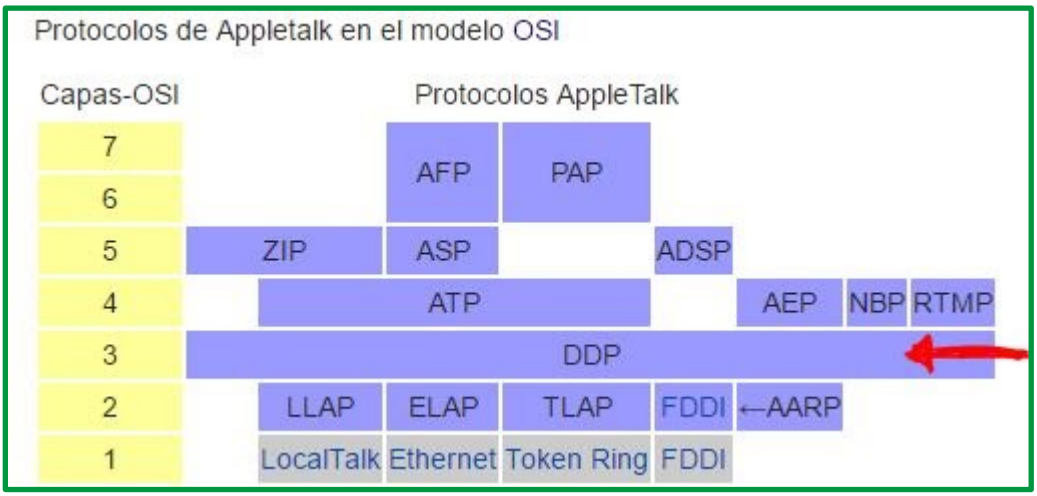


Figure 67. Análisis protocolo AppleTalk referente a capa OSI

Servicio de red sin conexión (CLNS/DECNet)

CLNS (Servicio No Orientado a Conexión), en telecomunicaciones, es un servicio que establece la comunicación entre entidades sin necesidad de establecer una conexión entre ellas. Cuando una entidad tiene información para transmitir, sencillamente la envía, (tramas, paquetes, bloques, etc.).

Funcionamiento

El proveedor trata cada objeto de información de forma independiente y autónoma, incluso aunque se trate de un conjunto de objetos pertenecientes al mismo mensaje. El usuario confía simplemente en que cada objeto ha de llegar a su destino más pronto o más tarde. Los servicios orientado y no orientado a conexión, se suelen asimilar con los servicios telefónico y postal respectivamente. El sistema telefónico es un ejemplo de servicio orientado a conexión, mientras que el sistema postal es un servicio no orientado a conexión. Esta analogía es perfectamente aplicable a la funcionalidad y a la lógica de los servicios CONS y CLNS.

DECnet.

Es un conjunto de protocolos desarrollado por Digital Equipment Corporation para interconectar ordenadores de tal manera que los usuarios pueden compartir programas, archivos de datos y dispositivos de terminales remotos. Actualmente se encuentra en la fase V, desarrollada por Digital y OSI.

NetBIOS y NetBEUI

NetBIOS (Network Basic Input/Output System) es un protocolo que permite que se comuniquen aplicaciones en diferentes ordenadores dentro de una LAN. Fue desarrollado en principio para las redes de ordenadores personales IBM y después fue adoptado por Microsoft. No permite por sí mismo un mecanismo de enrutamiento por lo que no es adecuado para redes de área extensa (MAN), en las que se deberá usar otro protocolo para el transporte de los datos. Una de las desventajas de NetBIOS es que no proporciona un marco estándar o formato de datos para la transmisión.

NetBEUI o Interfaz de Usuario para NetBIOS (NetBIOS Extended User Interface) es una versión mejorada de NetBIOS que permite el formato de la información en una transmisión de datos, aunque tampoco soporta el enrutamiento a otras redes, debiendo establecerse otros protocolos (IPX o TCP/IP). Se suele instalar NetBEUI y TCP/IP en cada estación de trabajo de modo que el servidor utilice NetBEUI para la comunicación dentro de la LAN y TCP/IP para la comunicación hacia afuera de la LAN.

PROVEEDOR DE SERVICIO DE INTERNET.

El papel de ISP

La mayoría de las compañías u organizaciones obtiene sus bloques de direcciones IPv4 de un ISP. Un ISP generalmente suministrará una pequeña cantidad de direcciones IPv4 utilizables (6 ó 14) a sus clientes como parte de los servicios. Se pueden obtener bloques mayores de direcciones de acuerdo con la justificación de las necesidades y con un costo adicional por el servicio.

En cierto sentido, el ISP presta o alquila estas direcciones a la organización. Si se elige cambiar la conectividad de Internet a otro ISP, el nuevo ISP suministrará direcciones de los bloques de direcciones que ellos poseen, y el ISP anterior devuelve los bloques prestados a su asignación para prestarlos nuevamente a otro cliente.

Servicios ISP

Para tener acceso a los servicios de Internet, tenemos que conectar nuestra red de datos a Internet usando un Proveedor de Servicios de Internet (ISP).

Los ISP poseen sus propios conjuntos de redes internas de datos para administrar la conectividad a Internet y ofrecer servicios relacionados. Entre los servicios que un ISP generalmente ofrece a sus clientes se encuentran los servicios DNS, servicios de correo electrónico y un sitio Web. Dependiendo del nivel de servicio requerido y disponible, los clientes usan diferentes niveles de un ISP.

ISP Tiers

Los ISP son designados por una jerarquía basada en su nivel de conectividad a la backbone de Internet. Cada nivel inferior obtiene conectividad al backbone por medio de la conexión a un ISP de nivel superior, como se muestra en la figura.

Nivel 1

En la parte superior de la jerarquía de ISP están los ISP de nivel 1. Éstos son grandes ISP a nivel nacional o internacional que se conectan directamente al backbone de Internet. Los clientes de ISP de nivel 1 son ISP de menor nivel o grandes compañías y organizaciones. Debido a que se encuentran en la cima de la conectividad a Internet, ofrecen conexiones y servicios altamente confiables. Entre las tecnologías utilizadas como apoyo de esta confiabilidad se encuentran múltiples conexiones al backbone de Internet.

Las principales ventajas para los clientes de ISP de nivel 1 son la confiabilidad y la velocidad. Debido a que estos clientes están a sólo una conexión de distancia de Internet, hay menos oportunidades de que se produzcan fallas o cuellos de botella en el tráfico. La desventaja para los clientes de ISP de nivel 1 es el costo elevado.

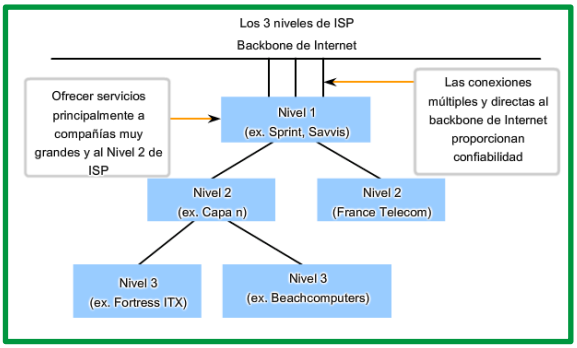


Figure 68. Nivel 1 ISP

Nivel 2

Los ISP de nivel 2 adquieren su servicio de Internet de los ISP de nivel 1. Los ISP de nivel 2 generalmente se centran en los clientes empresa. Los ISP de nivel 2 normalmente ofrecen más servicios que los ISP de los otros dos niveles. Estos ISP de nivel 2 suelen tener recursos de TI para ofrecer sus propios servicios como DNS, servidores de correo electrónico y servidores web. Otros servicios ofrecidos por los ISP de nivel 2 pueden incluir desarrollo y mantenimiento de sitios web, e-commerce/e-business y VoIP.

La principal desventaja de los ISP de nivel 2, comparados con los ISP de nivel 1, es el acceso más lento a Internet. Como los IPS de Nivel 2 están al menos a una conexión más lejos de la backbone de Internet, tienden a tener menor confiabilidad que los IPS de Nivel 1.

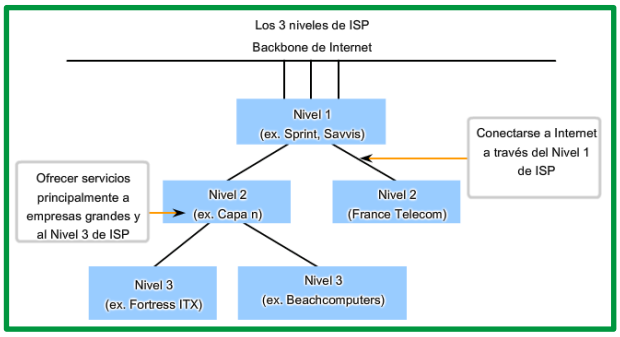


Figure 69. Nivel 2 ISP

Nivel 3

Los ISP de nivel 3 compran su servicio de Internet de los ISP de nivel 2. El objetivo de estos ISP son los mercados minoristas y del hogar en una ubicación específica. Típicamente, los clientes del nivel 3 no necesitan muchos de los servicios requeridos por los clientes del nivel 2. Su necesidad principal es conectividad y soporte.

Estos clientes a menudo tienen conocimiento escaso o nulo sobre computación o redes. Los ISP de nivel 3 suelen incluir la conectividad a Internet como parte del contrato de servicios de red y computación para los clientes. A pesar de que pueden tener un menor ancho de banda y menos confiabilidad que los proveedores de nivel 1 y 2, suelen ser buenas opciones para pequeñas y medianas empresas.

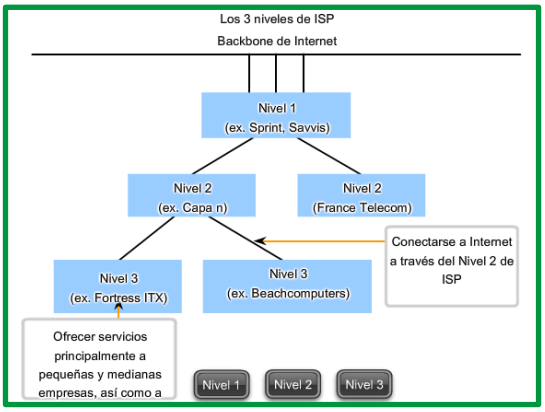


Figure 70. Nivel 3 ISP

QUIEN ASIGNAN LAS DIFERENTES DIRECCIONES IP

Una compañía u organización que desea acceder a la red mediante hosts desde Internet debe tener un bloque de direcciones públicas asignado. El uso de estas direcciones públicas es regulado y la compañía u organización debe tener un bloque de direcciones asignado. Esto es lo que sucede con las direcciones IPv4, IPv6 y multicast.

Autoridad de números asignados a Internet (IANA) (http://www.iana.net) es un soporte maestro de direcciones IP. Las direcciones IP multicast y las direcciones IPv6 se obtienen directamente de la IANA. Hasta mediados de los años noventa, todo el espacio de direcciones IPv4 era directamente administrado por la IANA. En ese entonces, se asignó el resto del espacio de direcciones IPv4 a otros diversos registros para que realicen la administración de áreas regionales o con propósitos particulares. Estas compañías de registro se llaman Registros regionales de Internet (RIR), como se muestra en la figura.

Global	IANA				
Registros de Internet regionales	**AfriNIC** Región de África	**APNIC** Asia/ Región del Pacífico	**LACNIC** Región de América Latina y el Caribe	**ARIN** Región de América del Norte	**RIPE NCC** Europa, Medio Oriente, Región de Asia Central

Figure 71. Entidades que supervisan la asignación de direcciones IP

Los principales registros son:

AfriNIC (African Network Information Centre) - Región de África http://www.afrinic.net

APNIC (Asia Pacific Network Information Centre) - Región de Asia/Pacífico http://www.apnic.net

ARIN (American Registry for Internet Numbers) - Región de Norte América http://www.arin.net

LACNIC (Registro de dirección IP de la Regional Latinoamericana y del Caribe) - América Latina y algunas islas del Caribe http://www.lacnic.net

RIPE NCC (Reseaux IP Europeans) - Europa, Medio Oriente y Asia Central http://www.ripe.net

Enlaces:

Búsqueda de direccionamiento IP: https://search.arin.net/rdap/

Tema 2: Direccionamiento IPv4/IPv6

El direccionamiento es una función clave de los protocolos de capa de Red que permite la transmisión de datos entre hosts de la misma red o en redes diferentes.

Protocolo de Internet versión 4 (IPv4) es la forma de direccionamiento IP utilizada habitualmente para identificar hosts en una red y utiliza un formato de 32 bits. El protocolo de Internet versión 6 (IPv6) es el estándar de dirección IP de última generación diseñado para sustituir el formato IPv4. IPv6 resuelve el problema de escasez de direcciones mediante el uso de direcciones de 128 bits en lugar de direcciones de 32 bits que se utilizaban en IPv4.

Puede realizar la revisión del estudio comparativos de IPv4 e IPV6 realizado por IBM en la dirección web https://www.ibm.com/docs/es/i/7.1?topic=6-comparison-ipv4-ipv6 .

Direccionamiento IP

Estructura Dirección IPv4

El Protocolo de Internet versión 4 (IPv4) ofrece direccionamiento jerárquico para paquetes que transportan datos.

Diseñar, implementar y administrar un plan de direccionamiento IPv4 efectivo asegura que las redes puedan operar de manera eficaz y eficiente. Cada dispositivo de una red debe ser definido en forma exclusiva. En la capa de red es necesario identificar los paquetes de la transmisión con las direcciones de origen y de destino de los dos sistemas finales. Con IPv4, esto significa que cada paquete posee una dirección de origen de 32 bits y una dirección de destino de 32 bits en el encabezado de Capa 3.

Para comprender el funcionamiento de los dispositivos en una red, debemos observar las direcciones y otros datos de la misma manera en que lo hacen los dispositivos: en ***notación binaria***. La ***notación binaria*** es una representación de la información mediante unos y ceros solamente. Las PC se comunican mediante datos binarios. Los datos binarios se pueden utilizar para representar muchas formas distintas de datos. Por ejemplo, al pulsar letras en un teclado, esas letras aparecen en la pantalla de una manera que el usuario puede leer y comprender. Sin embargo, la PC traduce cada letra a una serie de dígitos binarios para su almacenamiento y

transporte. Para traducir esas letras, la PC utiliza el Código Estadounidense Estándar para el Intercambio de Información (ASCII).

Mediante ASCII, la letra “A” se representa en forma de bit como “01000001”, mientras que la “a” minúscula se representa en forma de bit como “01100001”. Utilice el traductor de ASCII en la figura 1 para convertir los caracteres ASCII al sistema binario.

Si bien, por lo general, las personas no deben preocuparse por la conversión binaria de letras, es necesario comprender el uso del sistema binario para el direccionamiento IP. Cada dispositivo en una red se debe identificar de forma exclusiva mediante una dirección binaria. En redes IPv4, esta dirección se representa mediante una cadena de 32 bits (unos y ceros). A continuación, en la capa de red, los paquetes incluyen esta información de identificación única para los sistemas de origen y de destino. Por lo tanto, en una red IPv4, cada paquete incluye una dirección de origen de 32 bits y una dirección de destino de 32 bits en el encabezado de capa 3.

Para la mayoría de las personas, una cadena de 32 bits es difícil de interpretar e incluso más difícil de recordar. Por este motivo, representamos las direcciones IPv4 mediante el ***formato decimal punteado*** en lugar del binario. Esto significa que vemos a cada byte (octeto) como número decimal en el rango de 0 a 255. Para entender cómo funciona esto, es necesario conocer el proceso para la conversión de sistema binario a decimal.

Punto Decimal

Los patrones binarios que representan direcciones IPv4 son expresados con puntos decimales separando cada byte del patrón binario, llamado octeto, con un punto. Se le llama octeto debido a que cada número decimal representa un byte u 8 bits.

> ***Por ejemplo***: la dirección 10101100000100000000010000010100 es expresada en puntos decimales como 172.16.4.20.

Tenga en cuenta que los dispositivos usan la lógica binaria. El formato decimal punteado se usa para que a las personas les resulte más fácil utilizar y recordar direcciones.

Porciones de red y de host

En cada dirección IPv4, alguna porción de los bits de orden superior representa la dirección de red. En la Capa 3, se define una red como un grupo de hosts con patrones de bits idénticos en la porción de dirección de red de sus direcciones.

A pesar de que los 32 bits definen la dirección host IPv4, existe una cantidad variable de bits que conforman la porción de host de la dirección. El número de bits usado en esta porción del host determina el número de hosts que podemos tener dentro de la red.

Cada dispositivo de una red debe ser definido en forma exclusiva. En la capa de red es necesario identificar los paquetes de la transmisión con las direcciones de origen y de destino de los dos sistemas finales. Con IPv4, esto significa que cada paquete posee una dirección de origen de 32 bits y una dirección de destino de 32 bits en el encabezado de Capa 3.

Estas direcciones se usan en la red de datos como patrones binarios. Dentro de los dispositivos, la lógica digital es aplicada para su interpretación. Para quienes formamos parte de la red

humana, una serie de 32 bits es difícil de interpretar e incluso más difícil de recordar. Por lo tanto, representamos direcciones IPv4 utilizando el formato decimal punteada.

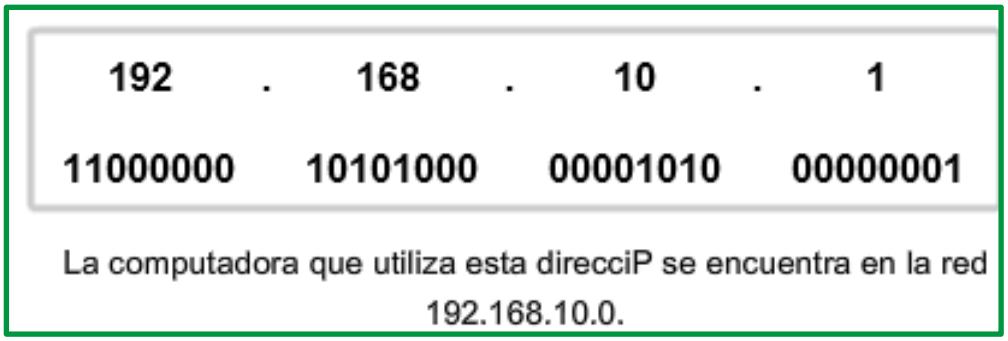


Figure 72. Ejemplo de Dirección IPv4

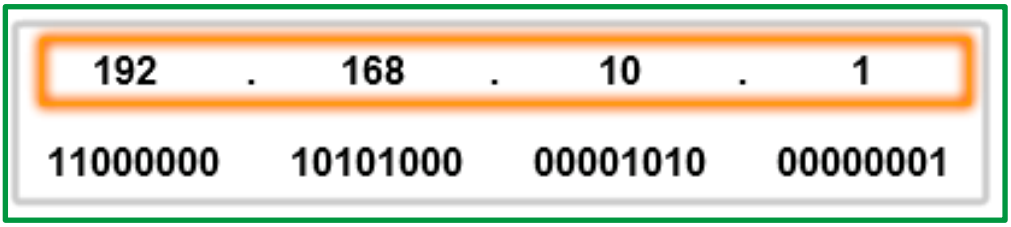


Figure 73. Dirección formato decimal Punteada

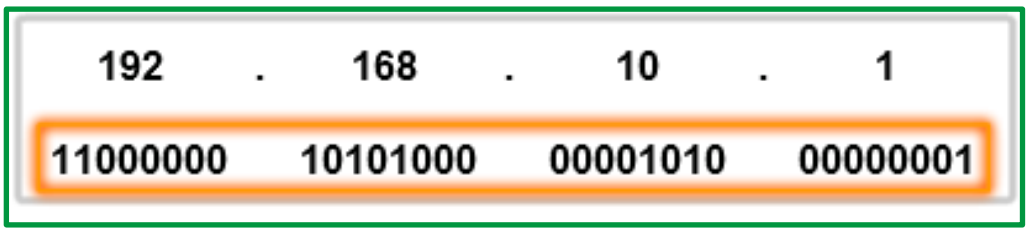


Figure 74. Dirección de 32 Bits

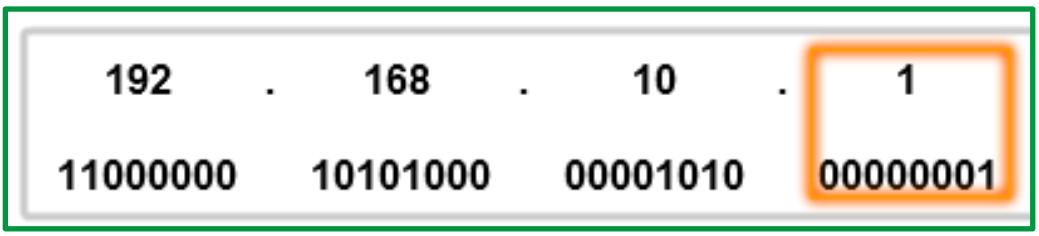


Figure 75. Host

En IPv4, las direcciones son números binarios de 32 bits. Sin embargo, para facilitar el uso por parte de las personas, los patrones binarios que representan direcciones IPv4 se expresan en formato decimal punteado. Esto primero se logra separando cada byte (8 bits) del patrón binario de 32 bits, llamado “octeto”, con un punto. Se le llama octeto debido a que cada número decimal representa un byte u 8 bits.

La dirección binaria:

11000000 10101000 00001010 00001010

Se expresa como decimal punteada de la siguiente manera:

192.168.10.10

En la figura se representa la dirección binaria 11000000 10101000 00001010 00001010

de 32 bits en octetos decimales punteados (192.168.10.10).

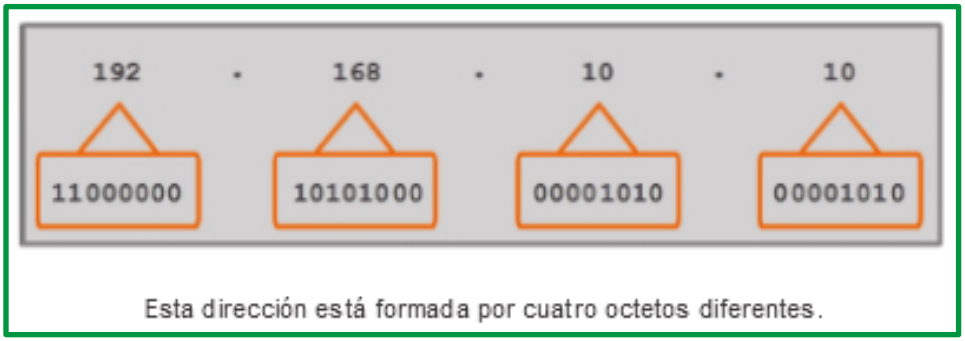


Figure 76. Octeto

Así mismo, es importante señalar que los tres primeros octetos de la ip 192.168.0.1 van a representar la parte correspondiente a la red.

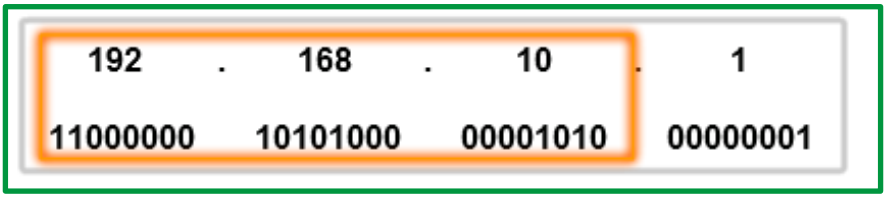


Figure 77. Red (192.168.10.0)

Para comprender el funcionamiento de un dispositivo en una red, es necesario considerar las direcciones y otros datos de la manera en que lo hace un dispositivo: en ***notación binaria***. Esto significa que es necesario ser hábil en la conversión de binario en decimal.

Los datos representados en el sistema binario pueden representar muchas formas diferentes de datos en la red humana. En este tema, se hace referencia al sistema binario por estar relacionado con el direccionamiento IPv4. Esto significa que vemos a cada byte (octeto) como número decimal en el rango de 0 a 255.

Notación de posición

Aprender a convertir el sistema binario a decimal requiere el conocimiento de los fundamentos matemáticos de un sistema de numeración denominado ***notación de posición***. “Notación de posición” significa que un dígito representa diferentes valores según la posición que ocupa. En un sistema de notación de posición, la base numérica se denomina “raíz”. En el sistema de base 10, la raíz es 10. En el sistema binario, se utiliza una raíz de 2. Los términos “raíz” y “base” se pueden utilizar de manera indistinta. Más específicamente, el valor que un dígito representa es el valor multiplicado por la potencia de la base o raíz representado por la posición que el dígito ocupa. Algunos ejemplos ayudarán a aclarar cómo funciona este sistema.

Para el número decimal 192, el valor que el 1 representa es ***1*10^2*** (1 multiplicado por 10 elevado a la segunda potencia). El 1 se encuentra en lo que comúnmente llamamos la posición "***100***". La notación de posición se refiere a esta posición como posición ***base^2*** porque la base o ***raíz es 10*** y la ***potencia es 2***. El 9 representa ***9*10^1*** (9 multiplicado por 10 elevado a la primera potencia). En la figura, se muestra la notación de posición para el número decimal 192.

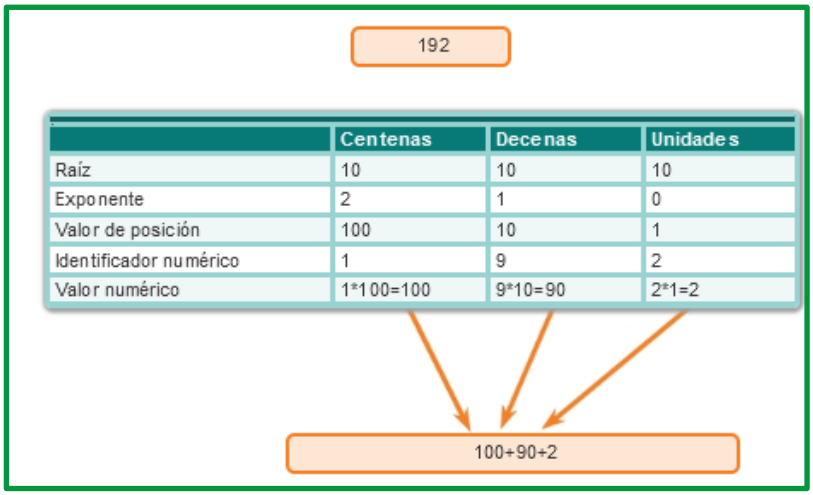


Figure 78. Ejemplo de notación de posición

Usando la notación de posición en el sistema de numeración con base 10, 192 representa:

192 = (1 * 10^2) + (9 * 10^1) + (2 * 10^0)

O

192 = (1 * 100) + (9 * 10) + (2 * 1)

Para el número decimal 245, el valor que el 2 representa es 2*10^2 (2 multiplicado por 10 elevado a la segunda potencia). El 2 se encuentra en lo que comúnmente llamamos la posición "100".

Usando la notación de posición en el sistema de numeración con base 10, 245 representa:

245 = (2 * 10^2) + (4 * 10^1) + (5 * 10^0)

o

245 = (2 * 100) + (4 * 10) + (5 * 1)

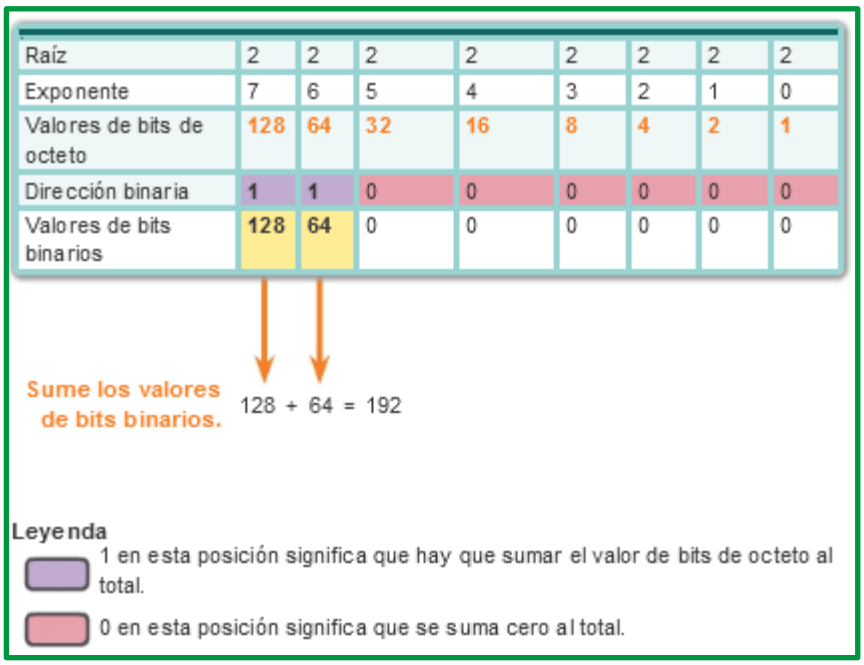
Sistema de numeración binaria

En el sistema de numeración binaria la ***raíz es 2***. Por lo tanto, cada posición representa aumentos en ***potencias de 2***. En números binarios de 8 bits, las posiciones representan estas cantidades:

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

El sistema de numeración de base 2 solo tiene dos dígitos: 0 y 1.

Cuando se interpreta un byte como un número decimal, se obtiene la cantidad que esa posición representa si el dígito es 1, y no se obtiene la cantidad si el dígito es 0.



En la figura, se ilustra la representación del número decimal 192 en sistema binario. Un 1 en una determinada posición significa que se agrega ese valor al total. Un 0 significa que no se agrega ese valor. El número binario 11000000 tiene un 1 en la posición 2^7 (valor decimal 128) y un 1 en la posición 2^6 (valor decimal 64). Los bits restantes son todos 0, de modo que no se agregan los valores decimales correspondientes. El resultado de agregar 128 + 64 es 192, el equivalente decimal de 11000000.

A continuación, se proporcionan dos ejemplos más:

Ejemplo 1: Un octeto compuesto solo por unos, **11111111**

Un 1 en cada posición significa que sumamos el valor para esa posición al total. Todos 1 significa que se incluyen los valores de cada posición en el total; por lo tanto, el valor de todos 1 en un octeto es 255.

1	+ 1	+ 1	+1	+ 1	+1	+1	+1 = 255
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**
128	64	32	16	8	4	2	1

Ejemplo 2: Un octeto compuesto solo por ceros, 00000000

Un 0 en cada posición indica que no se incluye el valor para esa posición en el total. Un 0 en cada posición produce un total de 0.

0	+ 0	+ 0	+0	+ 0	+ 0	+ 0	+ 0 = 0
0	0	0	0	0	0	0	0
128	64	32	16	8	4	2	1

Note en la figura que una combinación diferente de unos y ceros producirá un valor decimal diferente.

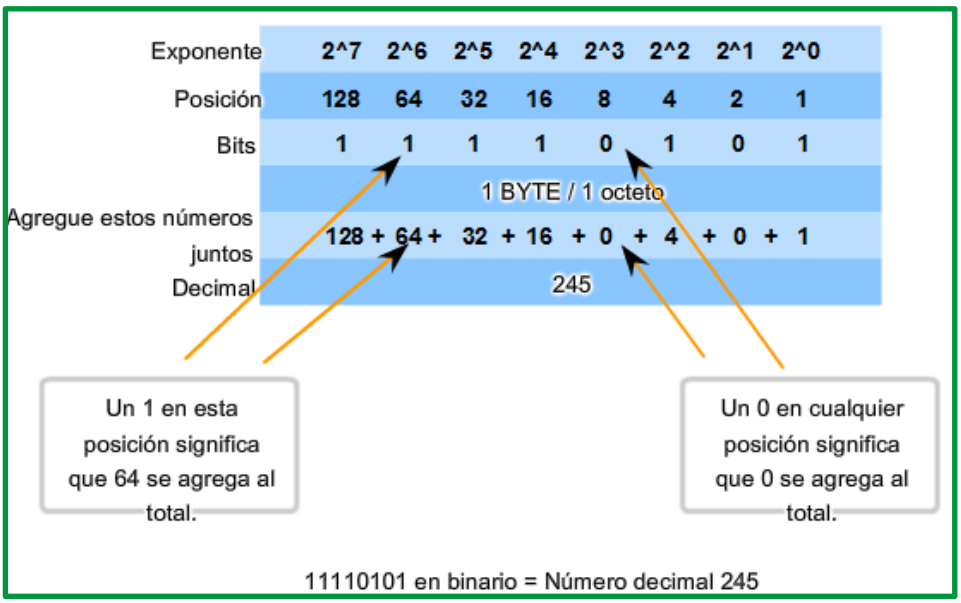


Figure 79. Conversión de binario a decimal

Cada octeto está compuesto por 8 bits y cada bit tiene un valor, 0 o 1. Los cuatro grupos de 8 bits tienen el mismo conjunto de valores válidos en el rango de 0 a 255 inclusive. El valor de cada ubicación de bits, de derecha a izquierda, es 1, 2, 4, 8, 16, 32, 64 y 128.

Determine el valor del octeto sumando los valores de las posiciones cada vez que haya un 1 binario presente.

- Si en esa posición hay un 0, no sume el valor.
- Si los 8 bits son 0, 00000000, el valor del octeto es 0.
- Si los 8 bits son 1, 11111111, el valor del octeto es 255 (128 + 64 + 32 + 16 + 8 + 4 + 2 + 1).
- Si los 8 bits están combinados, los valores se agregan juntos. Por ejemplo, el octeto 00100111 tiene un valor de 39 (32 + 4 + 2 + 1).

Por lo tanto, el valor de cada uno de los cuatro octetos puede ir de 0 a un máximo de 255.

Utilizando la dirección IPv4 de 32 bits 11000000101010000000101000001010, convierta la representación binaria en decimal punteada mediante los siguientes pasos:

Paso 1. Divida los 32 bits en 4 octetos.

Paso 2. Convierta cada octeto a decimal.

Paso 3. Agregue un "punto" entre cada decimal.

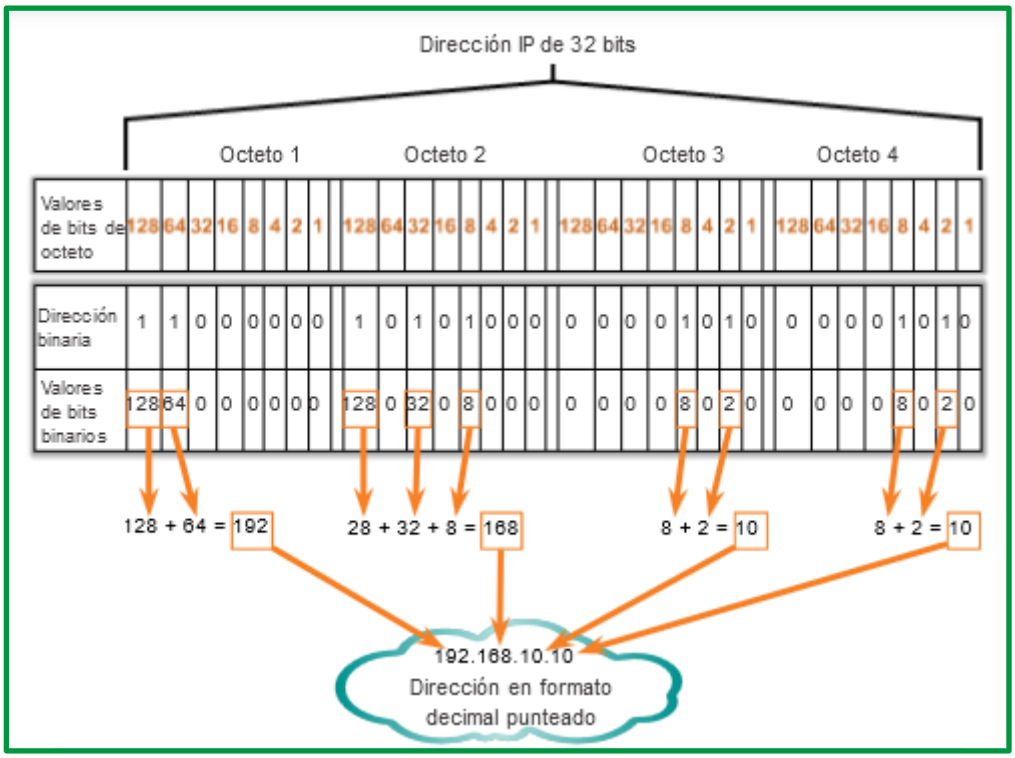


Figure 80. Conversión de una IPv4 de binario a decimal punteada

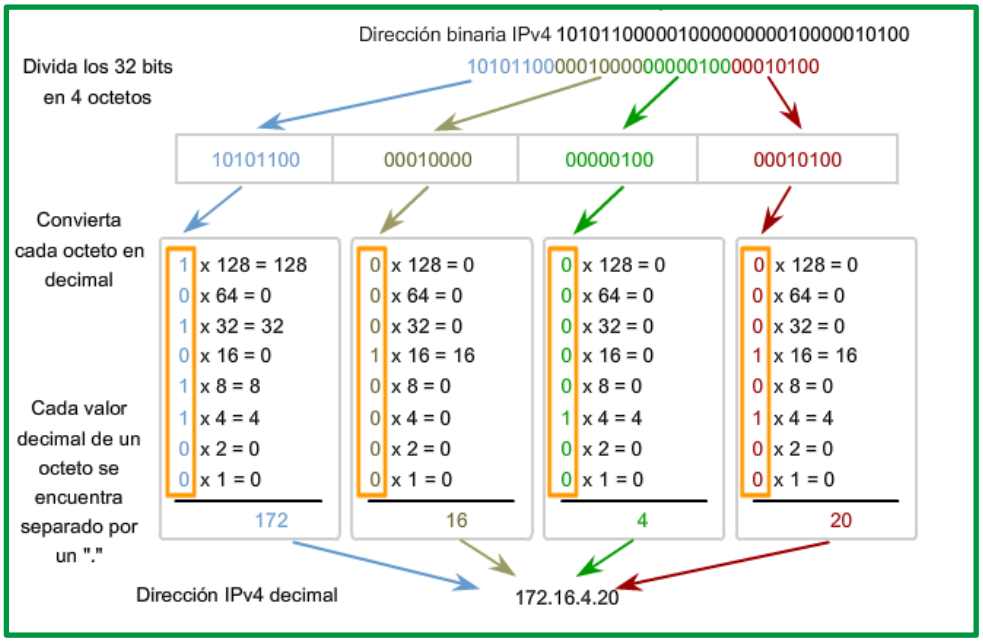


Figure 81.Ejemplo de conversión de una IPv4 de binario a decimal punteada

Se plantea para prática los siguientes ejercicios:

Ejercicio 1: 10000111 equivalente al decimal 135

Ejercicio 2: 10000000 equivalente al decimal 128

Ejercicio 3: 00010111 equivalente al decimal 23

Ejercicio 4: 01000101 equivalente al decimal 69

Ejercicio 5: 10011011 equivalente al número 155, se representa este grafica de resolución:

Valor decimal	155							
Raíz	2	2	2	2	2	2	2	2
Exponente	7	6	5	4	3	2	1	0
Posición	128	64	32	16	8	4	2	1
Bit	**1**	**0**	**0**	**1**	**1**	**0**	**1**	**1**
	Número binario							

Figure 82. Respuesta de ejercicio 5 - Convertir el binario 10011011 a notación decimal

Conversiones de decimal a binario:

Además de poder convertir de sistema binario a decimal, también es necesario comprender cómo convertir de decimal a binario.

Dado que representamos las direcciones IPv4 mediante el formato decimal punteado, solo es necesario analizar el proceso de conversión de valores binarios de 8 bits a valores decimales de 0 a 255 para cada octeto en una dirección IPv4.

Para comenzar el proceso de conversión, empezaremos determinando si el número decimal es igual a o mayor que nuestro valor decimal más grande representado por el bit más significativo. En la posición más alta, se determina si el número de octeto es igual o superior a 128. Si el número de octeto es inferior a 128, se coloca un 0 en la posición de bit para el valor decimal 128 y se avanza a la posición de bit para el valor decimal 64.

Si el número de octeto en la posición de bit para el valor decimal 128 es mayor o igual que 128, se coloca un 1 en la posición de bit para el valor decimal 128 y se resta 128 del número de octeto que se está convirtiendo. A continuación, comparamos el resto de esta operación con el siguiente valor más pequeño, 64. Continuamos este proceso para todas las posiciones de bits restantes.

En la figura siguiente, para ver el proceso de conversión de 168 al equivalente binario de 10101000 se aplica el siguiente esquema.

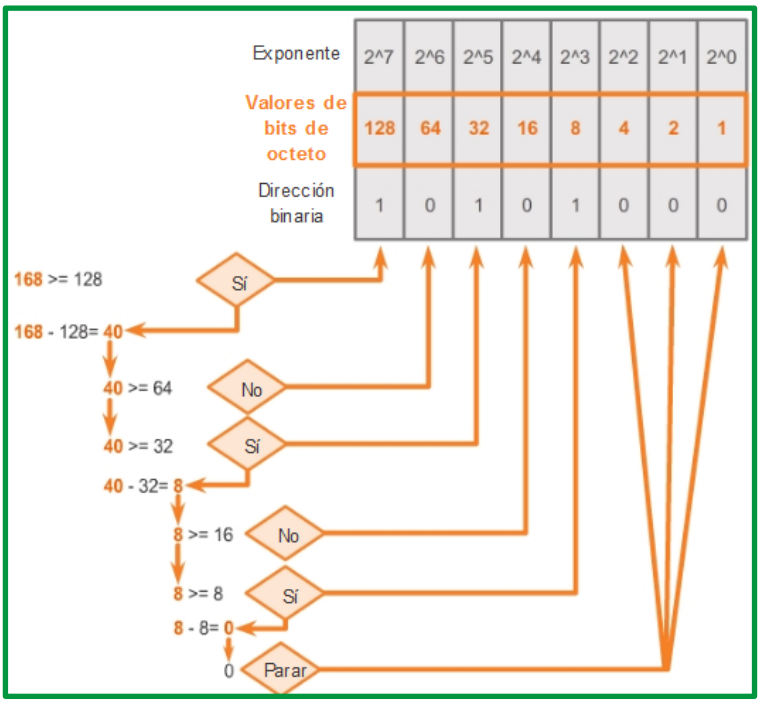


Figure 83. Conversión del número 168 de notación decimal a binario.

Ver la figura para obtener otro ejemplo. Se convierte 172 en 10101100.

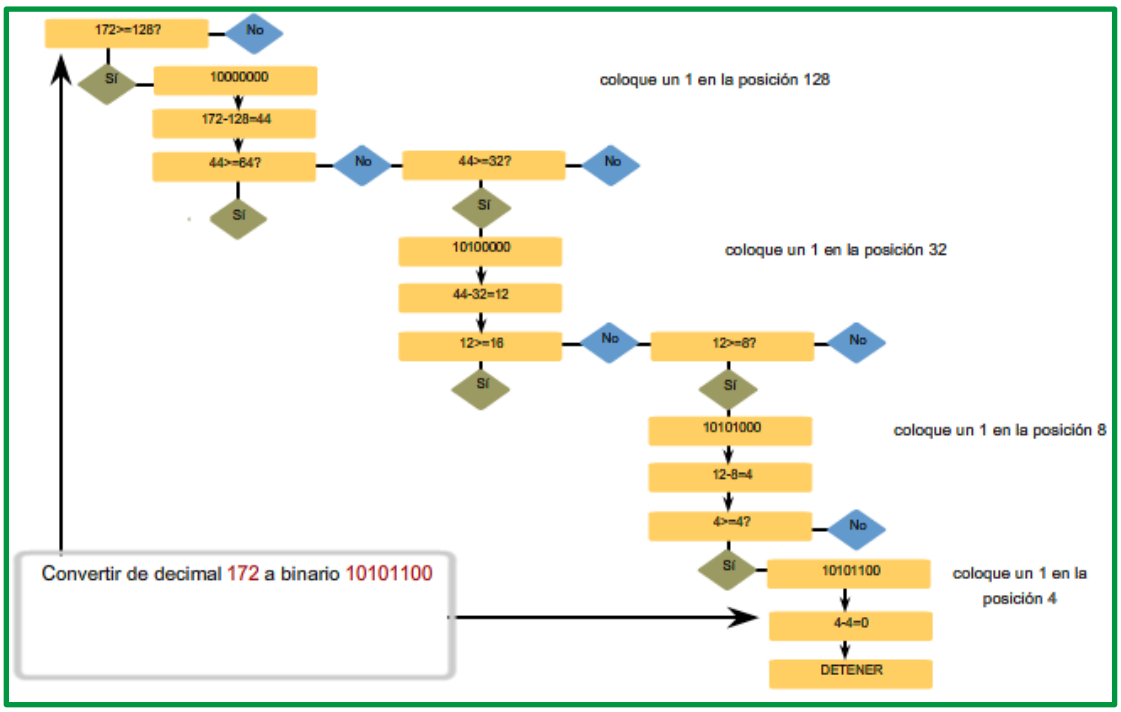


Figure 84. Proceso de conversión del decimal 172 a binario 10101100

Pasos de conversión para conocer cómo se convierte una dirección IP en binaria. 172.16.420

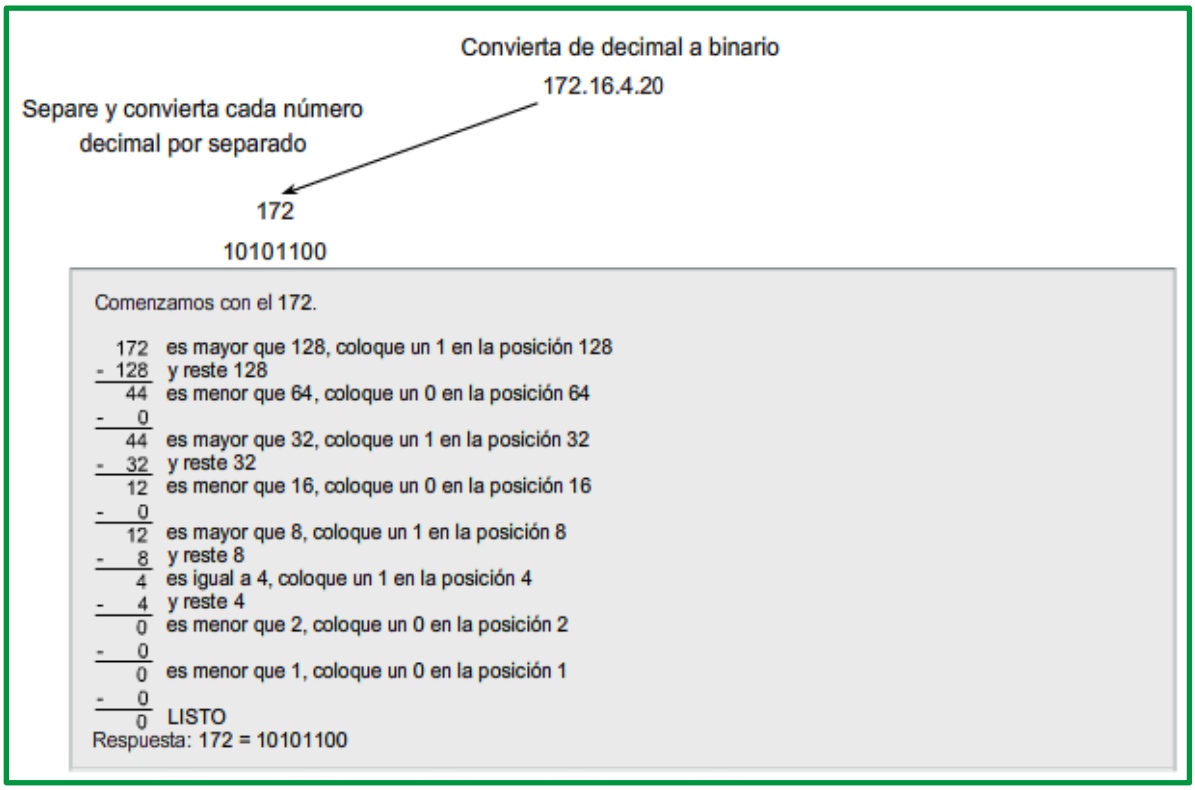


Figure 85. Paso 1

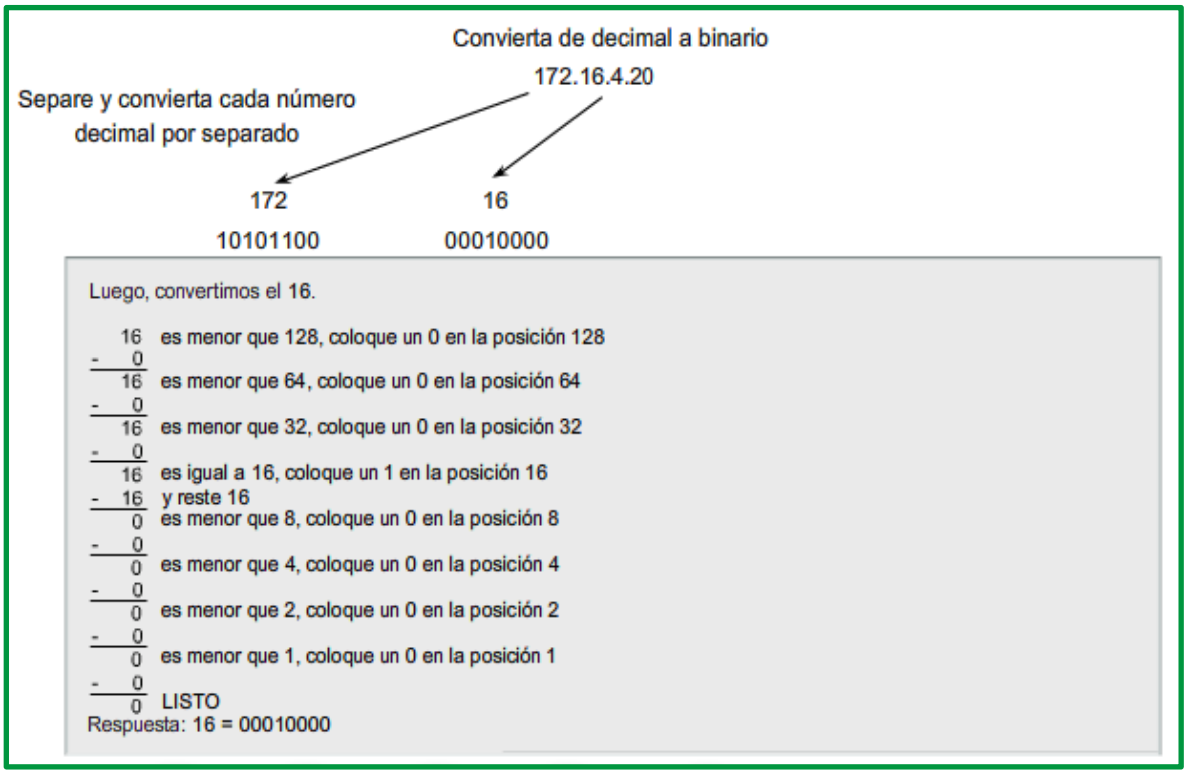


Figure 86. Paso 2

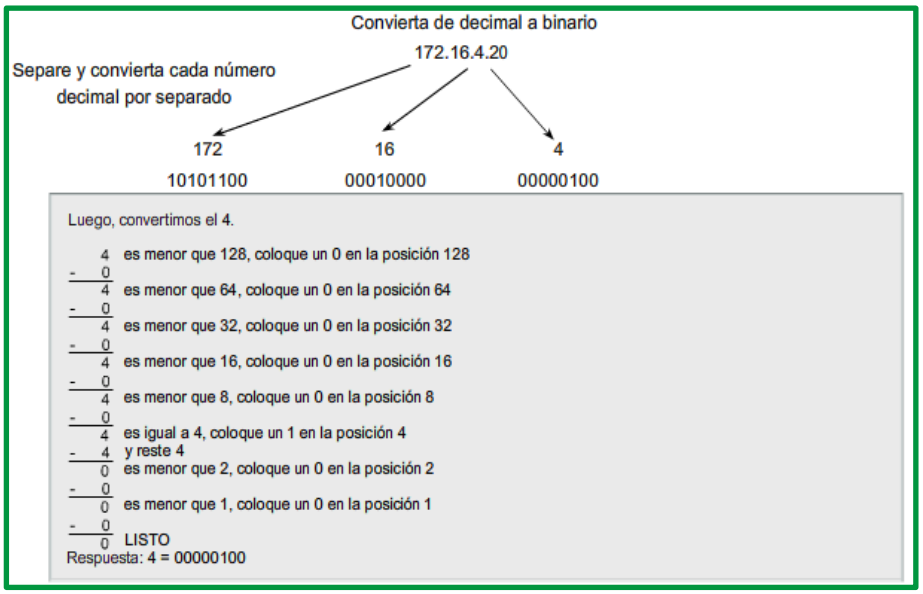


Figure 87. Paso 3

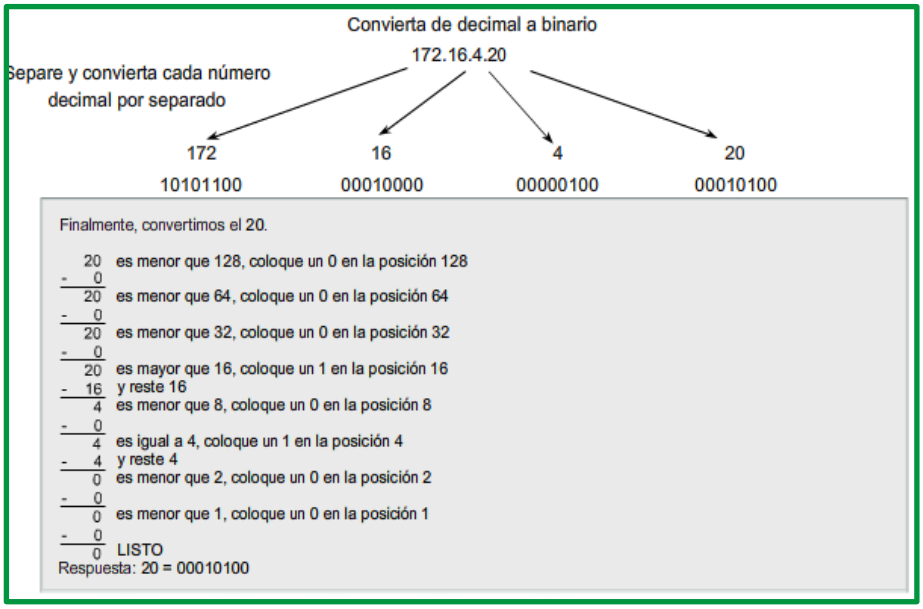


Figure 88. Paso 4

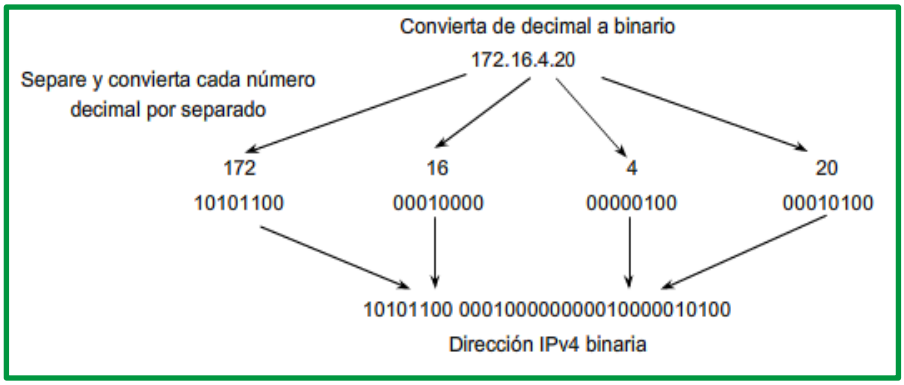
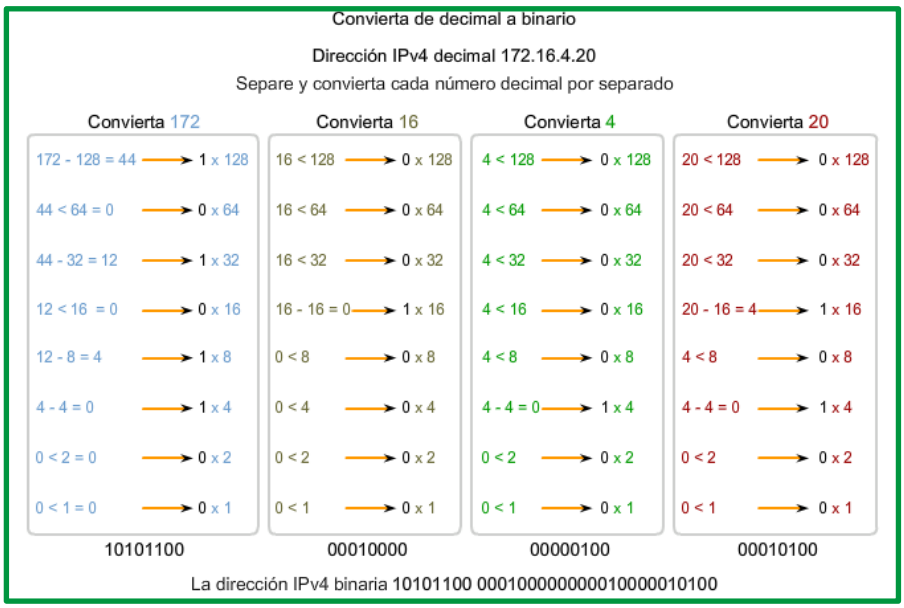


Figure 89. Resultado de conversión

La figura siguiente se resume la conversión completa de 172.16.4.20 de notación decimal punteada a notación binaria.



A continuación, se detallan pasos para convertir de decimal a binario 192.168.10.10

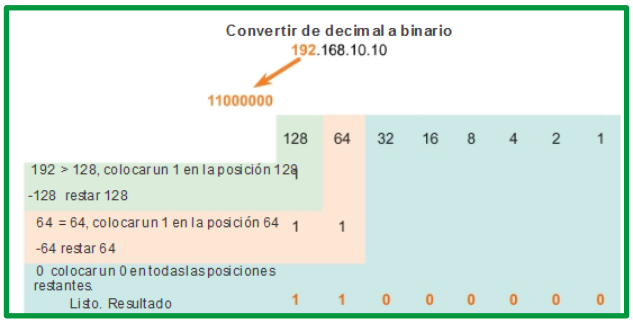


Figure 90. Paso 1

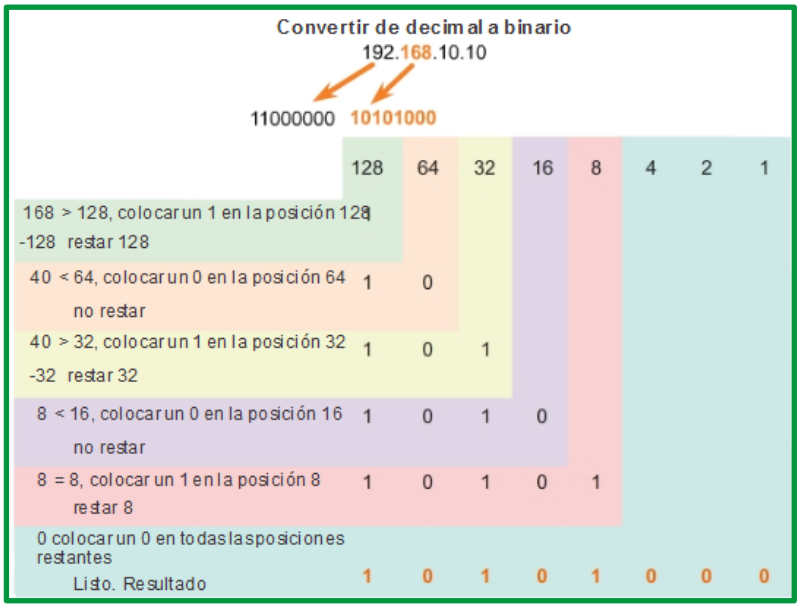


Figure 91. Paso 2

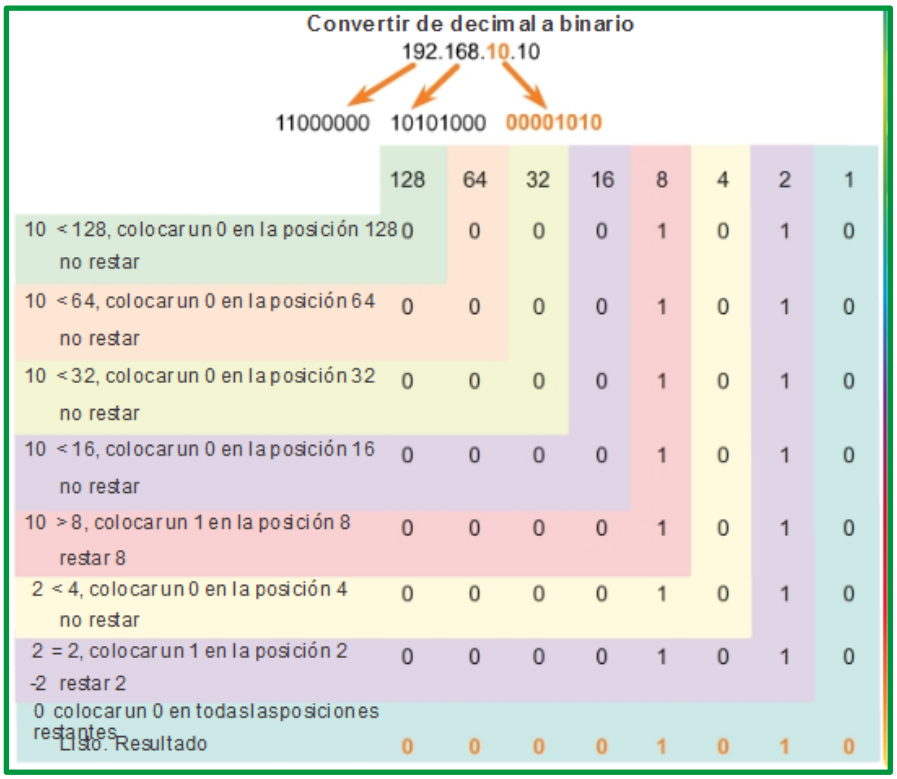


Figure 92. Paso 3

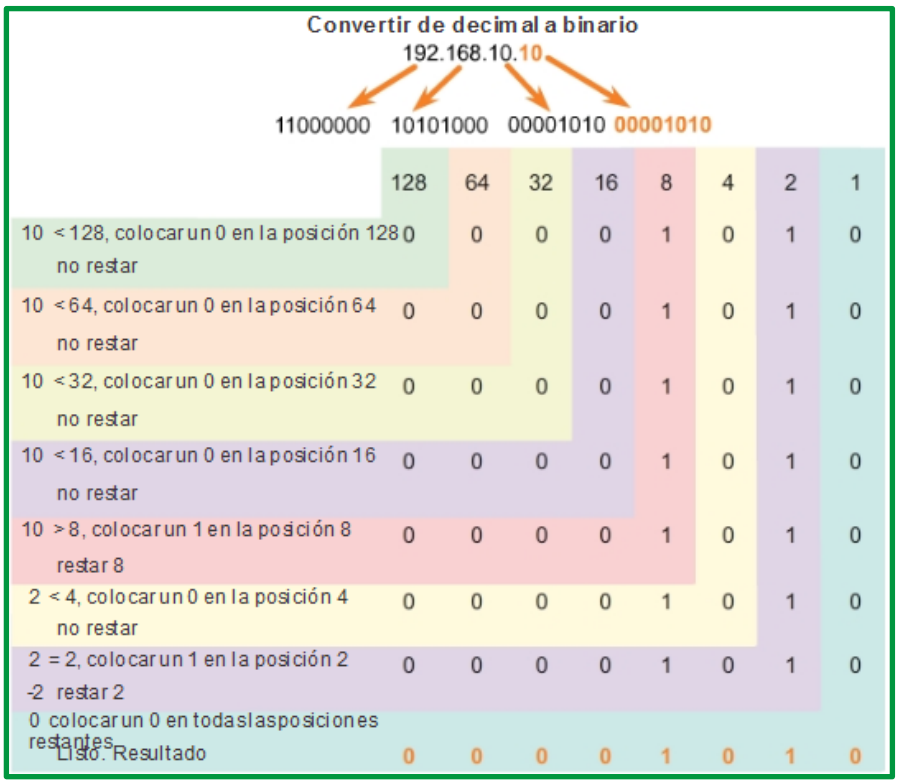


Figure 93. Paso4

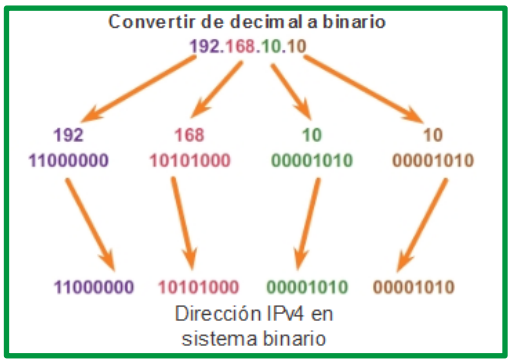


Figure 94. Resultado de conversión

Se plantea los siguientes ejercicios para práctica.

Ejercicio 1: **206** que es equivalente a binario **11001110**

Ejercicio 2: **150** que es equivalente a binario **10010110**

Ejercicio 3: **95** que es equivalente a binario **01011111**

Ejercicio 4: **95** que es equivalente a binario **00000101**

Ejercicio 5: **100** que es equivalente a binario **01100100**, se representa este gráfica de resolución:

Valor decimal	100							
Raíz	2	2	2	2	2	2	2	2
Exponente	7	6	5	4	3	2	1	0
Posición	128	64	32	16	8	4	2	1
Bit	**0**	**1**	**1**	**0**	**0**	**1**	**0**	**0**

Figure 95. Respuesta de ejercicio 5 - Convertir 100 de notación decimal a notación binario 01100100

Juegos con numero binarios: Una forma de aprender número binarios para el ámbito de redes es practicar, revise el link de juegos de cisco para practicar conversión de notación binaria a notación decimal y viceversa. https://learningcontent.cisco.com/games/binary/index.html

Mascara de subred IPv4

Es importante entender la notación binaria para determinar si dos hosts están en la misma red. Recuerde que una dirección IP es una dirección jerárquica que consta de dos partes: una porción de red y una porción de host. Pero al determinar la porción de red en comparación con la porción de host, es necesario analizar el stream de 32 bits, y no el valor decimal. Dentro del stream de 32 bits, una parte de los bits constituye la red y una porción de los bits constituye el host.

Los bits dentro de la porción de red de la dirección deben ser idénticos para todos los dispositivos que residen en la misma red. Los bits dentro de la porción de host de la dirección deben ser únicos para identificar un host específico dentro de una red. Independientemente de

si los números decimales entre dos direcciones IPv4 coinciden, si dos hosts tienen el mismo patrón de bits en la porción de red especificada del stream de 32 bits, esos dos hosts residen en la misma red.

¿Pero cómo saben los hosts qué porción de los 32 bits es red y qué porción es host? Esa tarea le corresponde a la máscara de subred.

Cuando se configura un host IP, se asigna una máscara de subred junto con una dirección IP. Como sucede con la dirección IP, la máscara de subred tiene una longitud de 32 bits. La máscara de subred identifica qué parte de la dirección IP corresponde a la red y cuál al host.

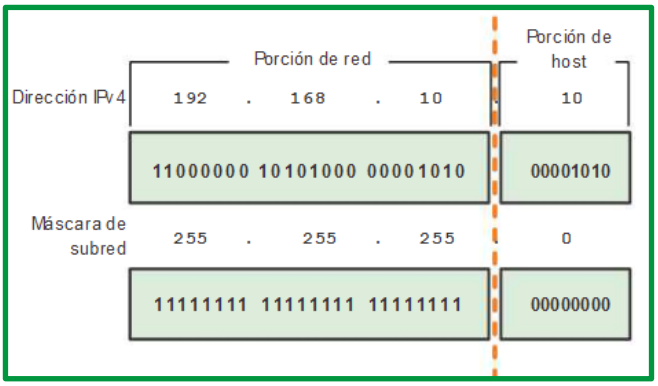


Figure 96. Mascara de Subred

La máscara de subred se compara con la dirección IP, de izquierda a derecha, bit por bit. Los 1 en la máscara de subred representan la porción de red, los 0 representan la porción de host. Como se muestra en la figura, la máscara de subred se crea al colocar un 1 binario en cada posición de bit que representa la porción de red y un 0 binario en cada posición de bit que representa la porción de host. Se debe tener en cuenta que la máscara de subred no contiene en efecto la porción de red o de host de una dirección IPv4, sino que simplemente le dice a la PC dónde buscar estas porciones en una dirección IPv4 dada.

Como sucede con las direcciones IPv4, la máscara de subred se representa en formato decimal punteado por cuestiones de facilidad de uso. La máscara de subred se configura en un dispositivo host, junto con la dirección IPv4, y es necesaria para que el host pueda determinar a qué red pertenece. En la figura siguiente se muestran las máscaras de subred válidas para un octeto IPv4.

Valor de subred	Valor de bit							
	128	64	32	16	8	4	2	1
255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

Figure 97. Mascara de subred válidas

Prefijos de red

La duración de prefijo es otra forma de expresar la máscara de subred. La duración de prefijo es la cantidad de bits establecidos en 1 en la máscara de subred. Se escribe en "notación con barras", una "/" seguida de la cantidad de bits establecidos en 1. Por ejemplo, si la máscara de subred es 255.255.255.0, hay 24 bits establecidos en 1 en la versión binaria de la máscara de subred, de modo que la duración de prefijo es 24 bits o /24. El prefijo y la máscara de subred son diferentes formas de representar lo mismo, la porción de red de una dirección.

No siempre se asigna un prefijo /24 a las redes. El prefijo asignado puede variar de acuerdo con la cantidad de hosts de la red. Tener un número de prefijo diferente cambia el rango de host y la dirección de broadcast para cada red.

En las ilustraciones, se muestran distintos prefijos que utilizan la misma dirección 10.1.1.0. En la figura se ilustran los prefijos /24 /25 /26 /27 /28.

Dirección de red	10.1.1.0/24	10.1.1.00000000
Primera dirección de host	10.1.1.1	10.1.1.00000001
Última dirección de host	10.1.1.254	10.1.1.11111110
Dirección de broadcast	10.1.1.255	10.1.1.11111111
Cantidad de hosts: 2^8 – 2 = 254 hosts		

Dirección de red	10.1.1.0/25	10.1.1.00000000
Primera dirección de host	10.1.1.1	10.1.1.00000001
Última dirección de host	10.1.1.126	10.1.1.01111110
Dirección de broadcast	10.1.1.127	10.1.1.01111111
Cantidad de hosts: 2^7 – 2 = 126 hosts		

Dirección de red	10.1.1.0/26	10.1.1.00000000
Primera dirección de host	10.1.1.1	10.1.1.00000001
Última dirección de host	10.1.1.62	10.1.1.00111110
Dirección de broadcast	10.1.1.63	10.1.1.00111111
Cantidad de hosts: 2^6 – 2 = 62 hosts		

Figure 98. Prefijos de red /24 /25 /26 de la dirección ip 10.1.1.0

	Decimal punteada	Bits importantes mostrados en sistema binario
Dirección de red	10.1.1.0/27	10.1.1.00000000
Primera dirección de host	10.1.1.1	10.1.1.00000001
Última dirección de host	10.1.1.30	10.1.1.00011110
Dirección de broadcast	10.1.1.31	10.1.1.00011111
Cantidad de hosts: 2^5 – 2 = 30 hosts		

Dirección de red	10.1.1.0/28	10.1.1.00000000
Primera dirección de host	10.1.1.1	10.1.1.00000001
Última dirección de host	10.1.1.14	10.1.1.00001110
Dirección de broadcast	10.1.1.15	10.1.1.00001111
Cantidad de hosts: 2^4 – 2 = 14 hosts		

Figure 99. Prefijos de red /27 /28 de la dirección ip 10.1.1.0

Observe que la dirección de red puede permanecer igual, pero el rango de host y la dirección de broadcast son diferentes para las diferentes duraciones de prefijos. En las ilustraciones, puede ver que la cantidad de hosts que se pueden direccionar en la red también cambia.

Por ejemplo: en 172.16.4.0 /24, /24 es la longitud de prefijo e indica que los primeros 24 bits son la dirección de red. Esto deja a los 8 bits restantes, el último octeto, como la porción de host. La máscara de subred consta de 32 bits, al igual que la dirección, y utiliza unos y ceros para indicar cuáles bits de la dirección son bits de red y cuáles bits son bits de host.

Utilización de diferentes prefijos para la red 172.16.4.0

Red	Dirección de red	Rango de host	Dirección de broadcast
172.16.4.0 /24	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
172.16.4.0 /25	172.16.4.0	172.16.4.1 - 172.16.4.126	172.16.4.127
172.16.4.0 /26	172.16.4.0	172.16.4.1 - 172.16.4.62	172.16.4.63
172.16.4.0 /27	172.16.4.0	172.16.4.1 - 172.16.4.30	172.16.4.31

MISMA DIRECCIÓN DE RED PARA TODOS LOS PREFIJOS

DIFERENTE DIRECCIÓN DE BROADCAST PARA CADA PREFIJO

Figure 100. Ejemplos de prefijo de red de la dirección ip 172.16.4.0

TIPOS DE DIRECCIONES IPV4

Dentro del rango de direcciones de cada red IPv4, existen tres tipos de direcciones:

- ***Dirección de red***: La dirección en la que se hace referencia a la red.
- ***Dirección de broadcast***: Una dirección especial utilizada para enviar datos a todos los hosts de la red.
- ***Direcciones host***: Las direcciones asignadas a los dispositivos finales de la red.

Dirección de red

La dirección de red es una manera estándar de hacer referencia a una red. Por ejemplo: se podría hacer referencia a la red de la figura como "red 10.0.0.0". Ésta es una manera mucho más conveniente y descriptiva de referirse a la red que utilizando un término como "la primera red". Todos los hosts de la red 10.0.0.0 tendrán los mismos bits de red.

Dentro del rango de dirección IPv4 de una red, la dirección más baja se reserva para la dirección de red. Esta dirección tiene un 0 para cada bit de host en la porción de host de la dirección.

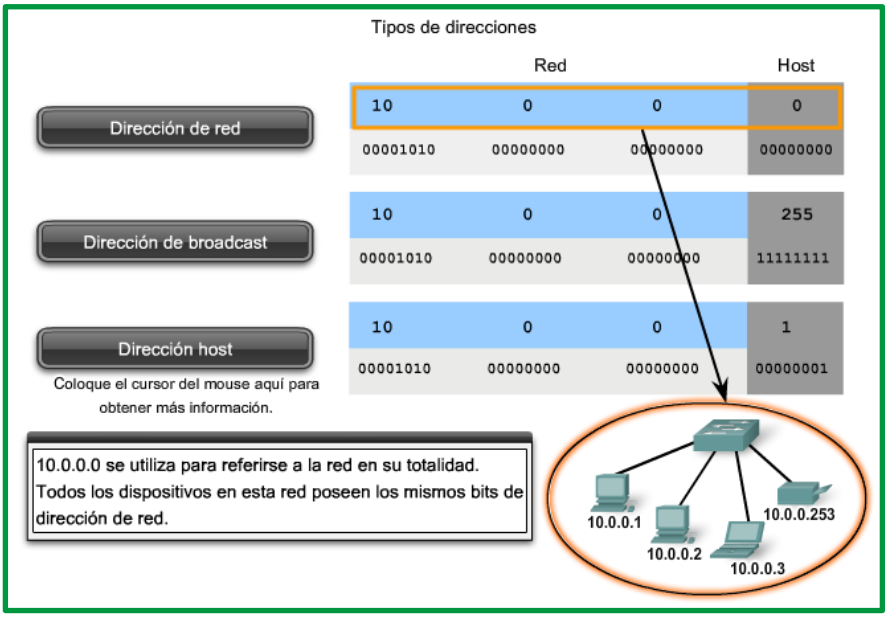


Figure 101. Dirección de red

Por ejemplo, la red que se muestra en la figura siguiente podría indicarse como la red 10.1.1.0, la red 10.1.1.0 255.255.255.0 o la red 10.1.1.0/24. Todos los hosts en la red 10.1.1.0/24 tendrán los mismos bits de porción de red.

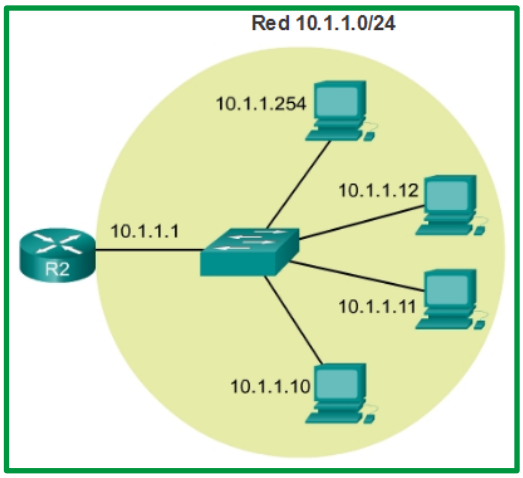


Figure 102. Red 10.1.1.0/24

Como se muestra en la figura, dentro del rango de direcciones IPv4 de una red, la primera dirección se reserva para la dirección de red. Esta dirección tiene un 0 para cada bit de host en la porción de host de la dirección. Todos los hosts dentro de la red comparten la misma dirección de red.

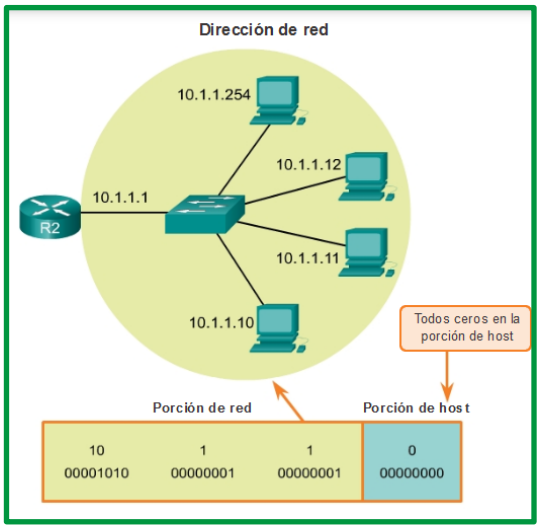


Figure 103. Dirección de Red

Dirección de broadcast

La dirección de broadcast IPv4 es una dirección especial para cada red que permite la comunicación a todos los hosts en esa red. Para enviar datos a todos los hosts de una red, un host puede enviar un solo paquete dirigido a la dirección de broadcast de la red, y cada host en la red que recibe este paquete procesa su contenido.

La dirección de broadcast utiliza la dirección más alta en el rango de la red. Ésta es la dirección en la cual los bits de la porción de host son todos 1. Para la red 10.0.0.0 con 24 bits de red, la dirección de broadcast sería 10.0.0.255. A esta dirección se la conoce como broadcast dirigido.

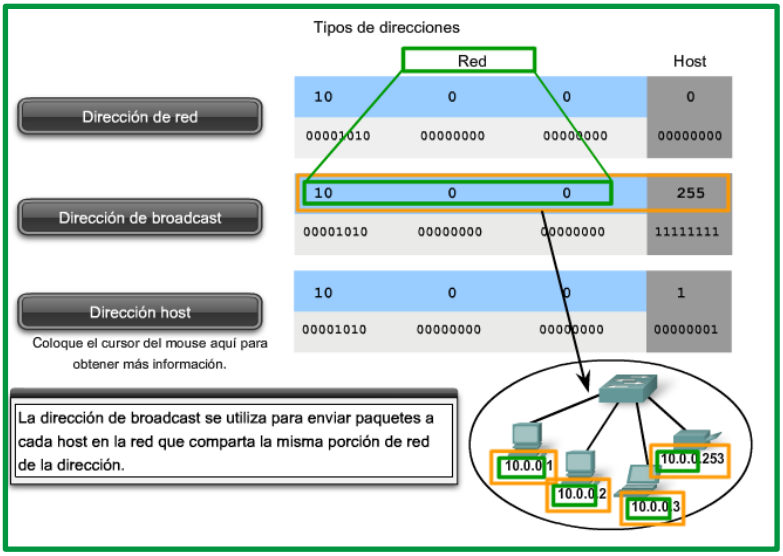


Figure 104. Dirección de Broadcast dirección 10.0.0.0

Todos 1 en un octeto en forma binaria es igual al número 255 en forma decimal. Por lo tanto, como se muestra en la figura siguiente, para la red 10.1.1.0/24, en la cual se utiliza el último octeto para la porción de host, la dirección de broadcast sería 10.1.1.255. Observe que la porción de host no siempre es un octeto entero. A esta dirección se la conoce como broadcast dirigido.

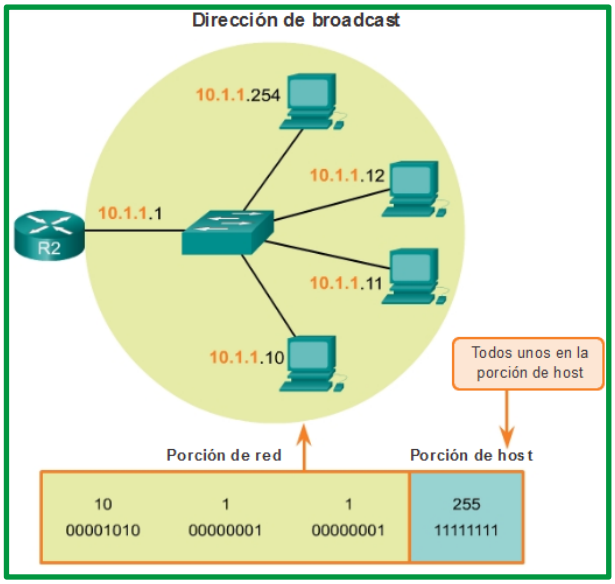


Figure 105. Dirección Broadcast red 10.1.1.254

Direcciones host

Cada dispositivo final requiere una dirección única para comunicarse en la red. En direcciones IPv4, los valores entre la dirección de red y la dirección de broadcast se pueden asignar a los dispositivos finales en una red. Como se muestra en las ilustraciones, esta dirección tiene cualquier combinación de bits 0 y bits 1 en la porción de host de la dirección, pero no puede contener todos bits 0 o todos bits 1.

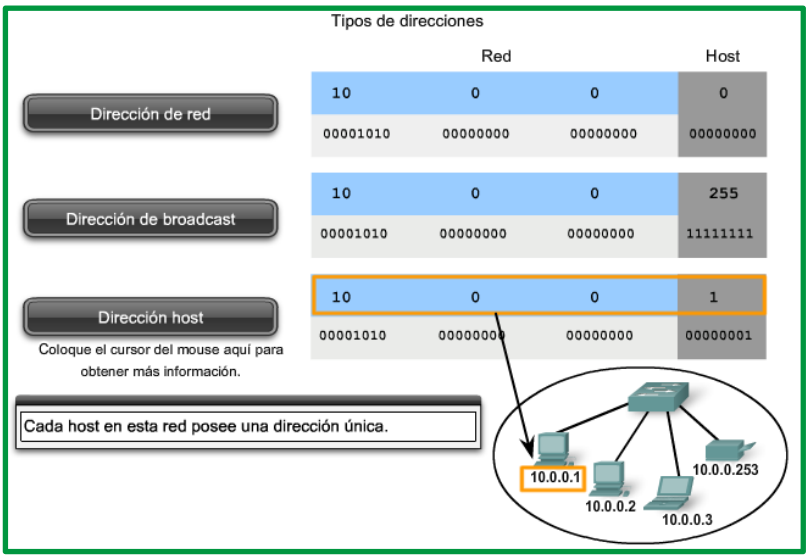


Figure 106. Dirección de host 10.0.0.1

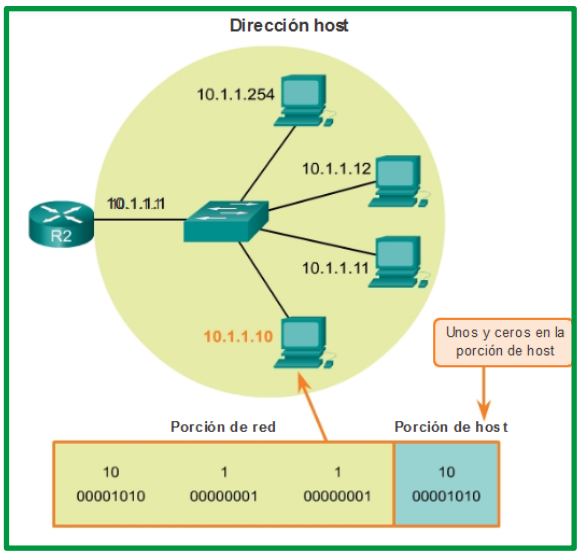


Figure 107. Dirección de host 10.1.1.10

ASIGNACION DE DIRECCIONES.

En las divisiones de red de ejemplo, se debe considerar el octeto de la dirección donde el prefijo divide la porción de red de la porción de host. En todos estos ejemplos, es el último octeto. A pesar de que esto es frecuente, el prefijo también puede dividir cualquiera de los octetos.

Para comenzar a comprender este proceso para determinar asignaciones de dirección, se desglosarán algunos ejemplos en datos binarios.

Observe la figura para obtener un ejemplo de la asignación de dirección para la red 172.16.20.0 /25.

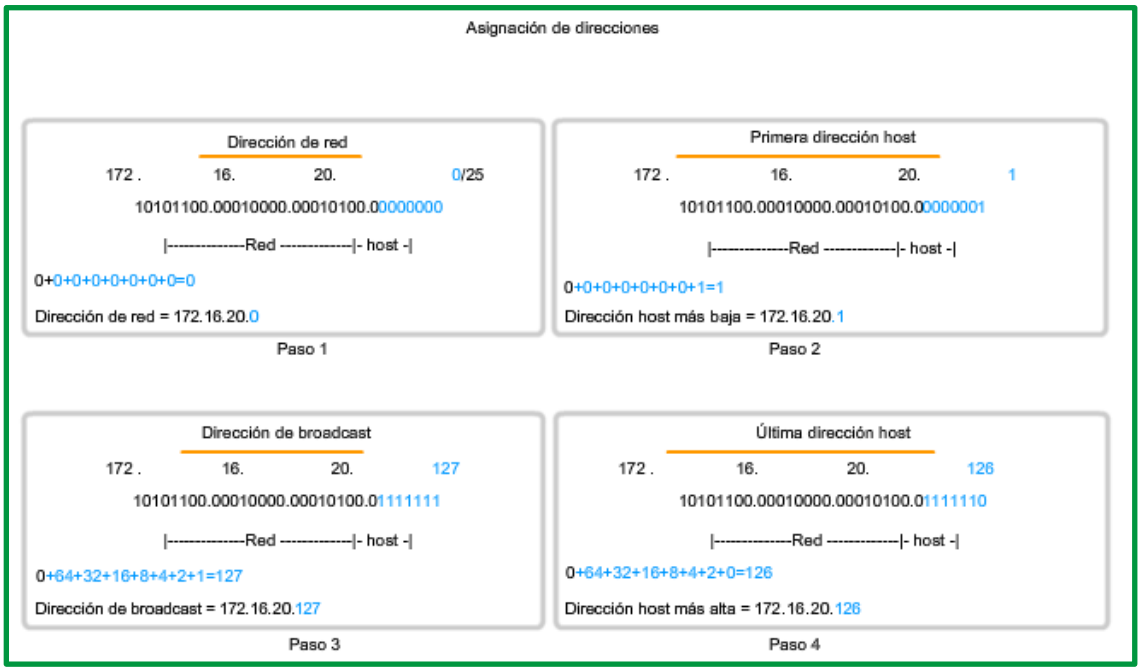


Figure 108. Asignaciones de Red

En el primer cuadro, se encuentra la representación de la dirección de red. Con un prefijo de 25 bits, los últimos 7 bits son bits de host. Para representar la dirección de red, todos estos bits de host son "0". Esto hace que el último octeto de la dirección sea 0. De esta forma, la dirección de red es 172.16.20.0 /25.

En el segundo cuadro, se observa el cálculo de la dirección host más baja. Ésta es siempre un número mayor que la dirección de red. En este caso, el último de los siete bits de host se convierte en "1". Con el bit más bajo en la dirección host establecido en 1, la dirección host más baja es 172.16.20.1.

El tercer cuadro muestra el cálculo de la dirección de broadcast de la red. Por lo tanto, los siete bits de host utilizados en esta red son todos "1". A partir del cálculo, se obtiene 127 en el último octeto. Esto produce una dirección de broadcast de 172.16.20.127.

El cuarto cuadro representa el cálculo de la dirección host más alta. La dirección host más alta de una red es siempre un número menor que la dirección de broadcast. Esto significa que el bit más bajo del host es un '0' y todos los otros bits '1'. Como se observa, esto hace que la dirección host más alta de la red sea 172.16.20.126.

Para asegurarse de que a todos los hosts en una red se les asigne una dirección IP única dentro de ese rango de red, es importante identificar la primera y la última dirección de host. Se pueden asignar direcciones IP dentro de este rango a los hosts dentro de una red.

Primera dirección de host

Como se observa en la figura, la porción de host de la primera dirección de host contiene todos bits 0 con un bit 1 que representa el bit de orden más bajo o el bit que está más a la derecha. Esta dirección es siempre un número mayor que la dirección de red. En este ejemplo, la primera dirección de host en la red 10.1.1.0/24 es 10.1.1.1. En muchos esquemas de direccionamiento, es común utilizar la primera dirección de host del router o la dirección de gateway predeterminado.

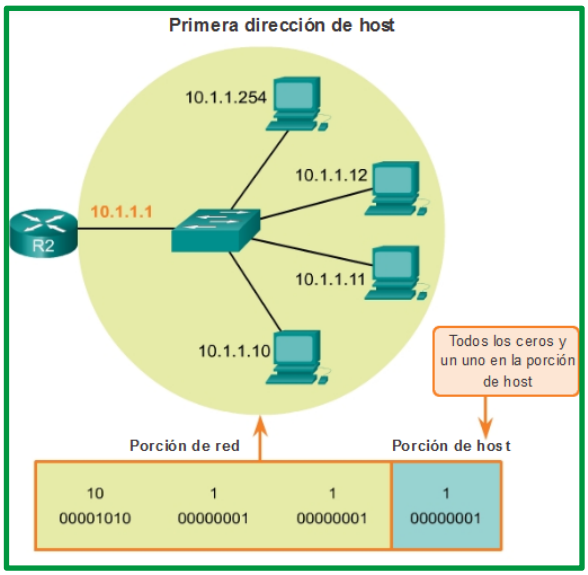


Figure 109. Ejemplo de primera dirección de host red 10.1.1.0/24

Última dirección de host

La porción de host de la última dirección de host contiene todos bits 1, con un bit 0 que representa el bit de orden más bajo o el bit que está más a la derecha. Esta dirección es siempre una menos que la dirección de broadcast. Como se observa en la figura, la última dirección de host en la red 10.1.1.0/24 es 10.1.1.254.

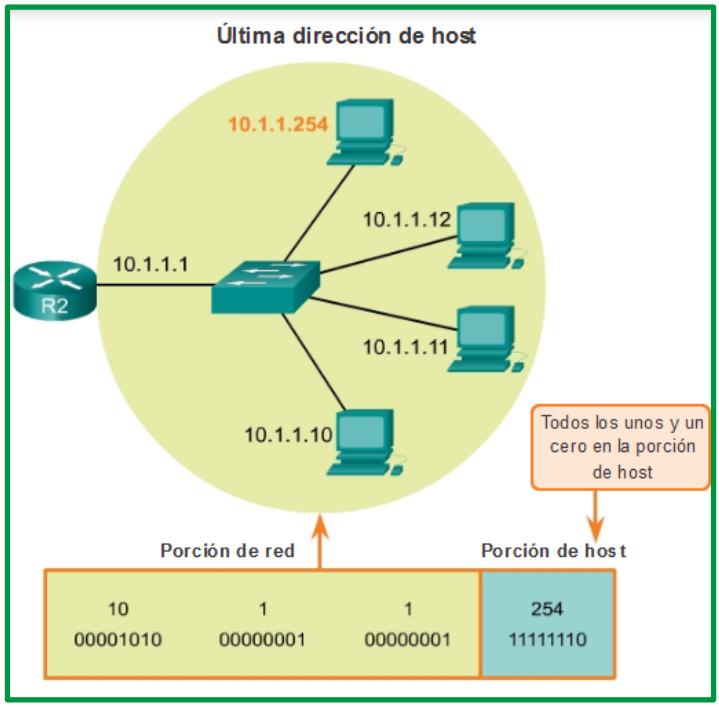


Figure 110. Ejemplo de ultima dirección de host red 10.1.1.0/24

Cuando se asigna una dirección IPv4 a un dispositivo, ese dispositivo utiliza la máscara de subred para determinar a qué dirección de red pertenece. La dirección de red es la dirección que representa todos los dispositivos en la misma red.

Al enviar datos de red, el dispositivo utiliza esta información para determinar si puede enviar paquetes localmente o si debe enviarlos a un gateway predeterminado para la entrega remota. Cuando un host envía un paquete, compara la porción de red de su propia dirección IP con la porción de red de la dirección IP de destino, sobre la base de las máscaras de subred. Si los bits de la red coinciden, tanto el host de origen como el de destino se encuentran en la misma red, y el paquete puede ser enviado localmente. Si no coinciden, el host emisor reenvía el paquete al gateway predeterminado para que se envíe a otra red.

La operación AND

AND es una de las tres operaciones binarias básicas que se utilizan en la lógica digital. Las otras dos son OR y NOT. Mientras que las tres se usan en redes de datos, AND se usa para determinar la dirección de red. Por lo tanto, sólo se tratará aquí la lógica AND. La lógica AND es la comparación de dos bits que produce los siguientes resultados:

- 1 AND 1 = 1

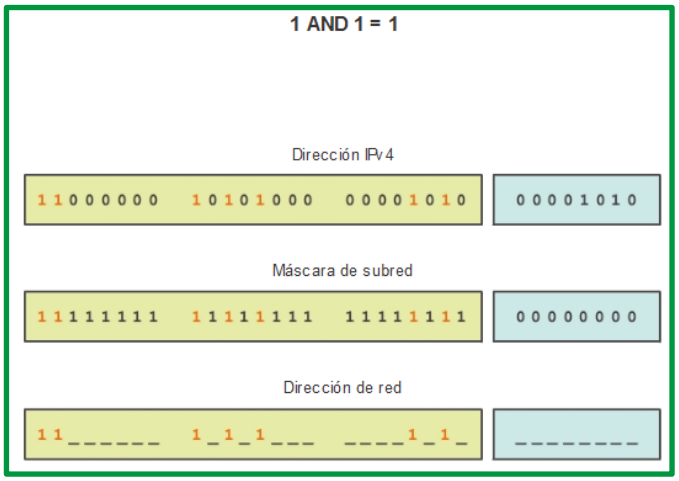


Figure 111. Operación 1 AND 1 = 1

- 0 AND 1 = 0

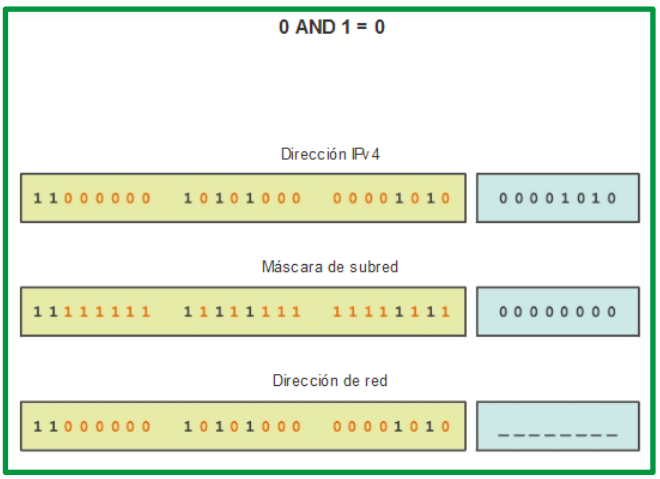


Figure 112. Operación 0 AND 1 = 0

- 0 AND 0 = 0

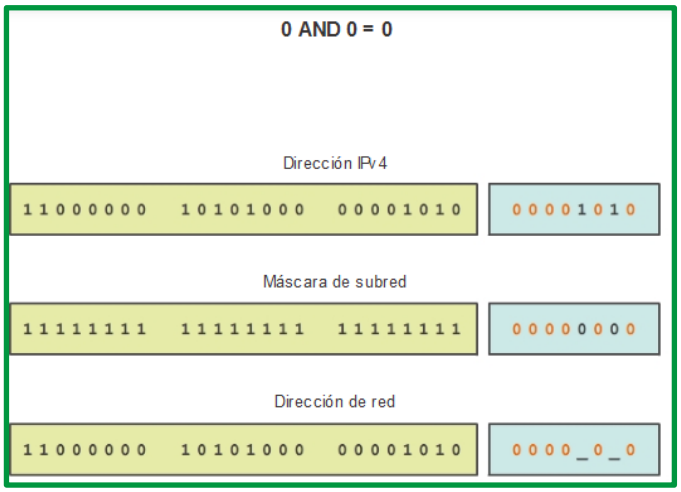


Figure 113. Operación 0 AND 0 = 0

- 1 AND 0 = 0

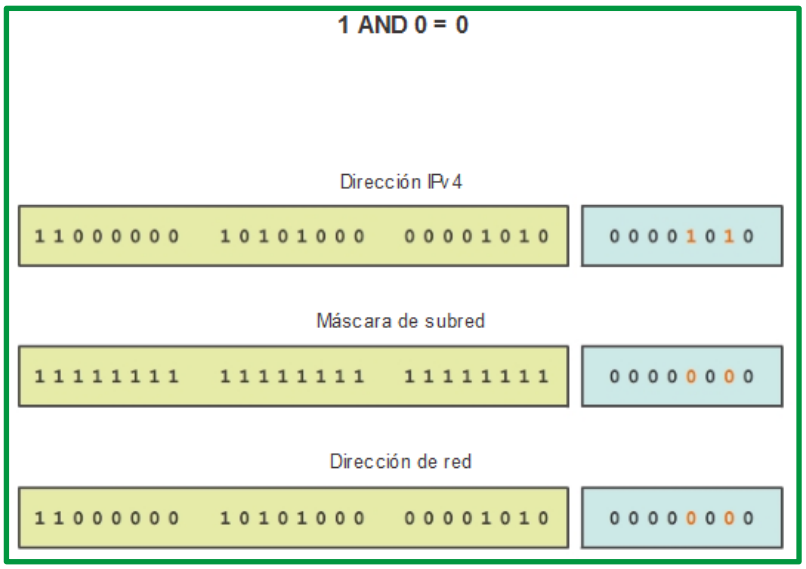


Figure 114. Figure 109. Operación 1 AND 0 = 0

Se aplica la lógica AND a la dirección de host IPv4, bit a bit, con su máscara de subred, para determinar la dirección de red a la cual se asocia el host. Cuando se aplica esta lógica AND bit a bit entre la dirección y la máscara de subred, el resultado que se produce es la dirección de red.

Si se aplica la lógica AND a cualquier bit de la dirección con valor de bit de 1 de la máscara de subred, da como resultado el valor de bit original de la dirección. Entonces, un 0 (de la dirección IPv4) AND 1 (de la máscara de subred) es 0. Un 1 (de la dirección IPv4) AND 1 (de la máscara de subred) es 1. Por lo tanto, el resultado de la aplicación de AND con un 0 en cualquier caso es 0. Estas propiedades de la operación AND se utilizan con la máscara de subred para “enmascarar” los bits de host de una dirección IPv4. Se aplica la lógica AND a cada bit de la dirección con el bit de máscara de subred correspondiente.

Debido a que todos los bits de la máscara de subred que representan bits de host son 0, la porción de host de la dirección de red resultante está formada por todos 0. Recuerde que una dirección IPv4 con todos 0 en la porción de host representa la dirección de red.

Asimismo, todos los bits de la máscara de subred que indican la porción de red son 1. Cuando se aplica la lógica AND a cada uno de estos 1 con el bit correspondiente de la dirección, los bits resultantes son idénticos a los bits de la dirección original.

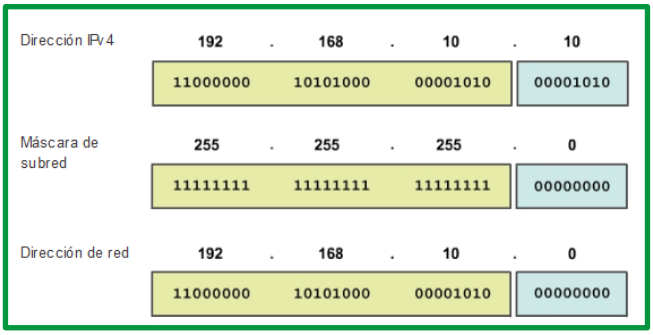


Figure 115. Dirección de red aplicando operación AND

Como se muestra en la ilustración, los bits 1 en la máscara de subred hacen que la porción de red de la dirección de red tenga los mismos bits que la porción de red del host. La porción de host de la dirección de red da como resultado todos 0.

En una dirección IP dada y su subred, se puede utilizar la operación AND para determinar a qué subred pertenece la dirección, así como qué otras direcciones pertenecen a la misma subred. Se debe tener en cuenta que, si dos direcciones están en la misma red o subred, se considera que son locales una respecto de la otra y, por consiguiente, pueden comunicarse directamente entre sí. Las direcciones que no se encuentran en la misma red o subred se consideran remotas respecto de sí y, por lo tanto, deben tener un dispositivo de capa 3 (como un router o un switch de capa 3) entre ellas para comunicarse.

En la verificación o resolución de problemas de red, con frecuencia es necesario determinar si dos hosts se encuentran en la misma red local. Es necesario tomar esta determinación desde el punto de vista de los dispositivos de red. Debido a una configuración incorrecta, un host puede encontrarse en una red que no era la planificada. Esto puede hacer que el funcionamiento parezca irregular, a menos que se realice el diagnóstico mediante el análisis de los procesos de aplicación de AND utilizados por el host.

Ejercicio de cálculo para practicar para evaluación. Calcule lo siguiente:

- Dirección de red
- Dirección broadcast
- Primera dirección host utilizable
- Última dirección host utilizable

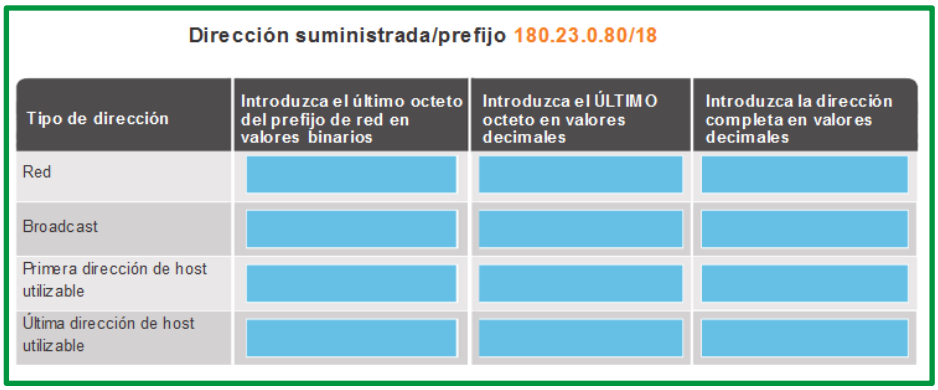


Figure 116. Ejercicio para realizar práctica de cálculo

Asignación dinámica

En las redes locales, es habitual que la población de usuarios cambie frecuentemente. Se agregan nuevos usuarios con computadoras portátiles, y esos usuarios requieren una conexión. Otros tienen estaciones de trabajo nuevas u otros dispositivos de red, como smartphones, que deben conectarse. En lugar de que el administrador de red asigne direcciones IP para cada estación de trabajo, es más simple que las direcciones IP se asignen automáticamente. Esto se realiza mediante un protocolo conocido como Protocolo de configuración dinámica de host (DHCP), como se muestra en la figura.

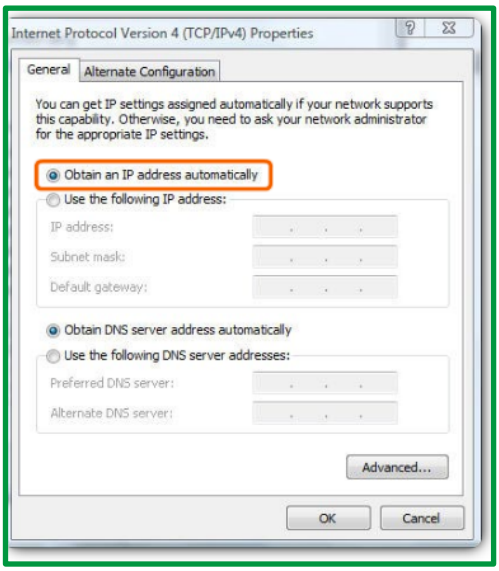


Figure 117. Asignación de Dirección IP por DHCP

El DHCP permite la asignación automática de información de direccionamiento, como una dirección IP, una máscara de subred, un gateway predeterminado y otra información de configuración. La configuración del servidor de DHCP requiere que se utilice un bloque de direcciones, denominado “conjunto de direcciones”, para la asignación a los clientes DHCP en una red. Las direcciones asignadas a este conjunto deben planificarse de modo que excluyan cualquier dirección estática que utilicen otros dispositivos.

DHCP es generalmente el método preferido para asignar direcciones IPv4 a los hosts de grandes redes, dado que reduce la carga para al personal de soporte de la red y prácticamente elimina los errores de entrada.

Otro beneficio de DHCP es que no se asigna de manera permanente una dirección a un host, sino que sólo se la "alquila" durante un tiempo. Si el host se apaga o se desconecta de la red, la dirección regresa al pool para volver a utilizarse. Esta función es muy útil para los usuarios móviles que entran y salen de la red.

Si se habilita DHCP en un dispositivo host, se puede utilizar el comando ipconfig para ver la información de la dirección IP que asigna el servidor de DHCP, como se muestra en la figura.

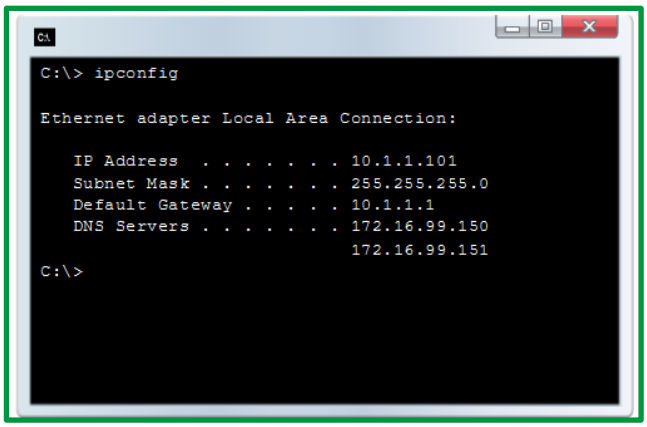


Figure 118. Verificación de IP con comando ipconfig en Windows

TIPOS DE COMUNICACIÓN

Unicast: El proceso por el cual se envía un paquete de un host a un host individual.

Broadcast: El proceso por el cual se envía un paquete de un host a todos los hosts de la red.

Multicast: El proceso por el cual se envía un paquete de un host a un grupo seleccionado de hosts, posiblemente en redes distintas.

Estos tres tipos de comunicación se usan con diferentes objetivos en las redes de datos. En los tres casos, se coloca la dirección IPv4 del host de origen en el encabezado del paquete como la dirección de origen.

Tráfico unicast

La comunicación unicast se usa para una comunicación normal de host a host, tanto en una red de cliente/servidor como en una red punto a punto. Los paquetes unicast utilizan la dirección host del dispositivo de destino como la dirección de destino y pueden enrutarse a través de una internetwork. Sin embargo, los paquetes broadcast y multicast usan direcciones especiales como la dirección de destino. Al utilizar estas direcciones especiales, los broadcasts están generalmente restringidos a la red local. El ámbito del tráfico multicast también puede estar limitado a la red local o enrutado a través de una internetwork.

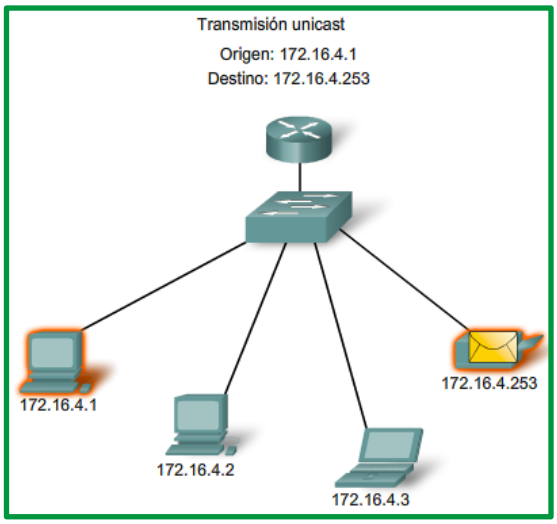


Figure 119. Trafico unicast

En una red IPv4, la dirección unicast aplicada a un dispositivo final se denomina “dirección de host”. En la comunicación unicast, las direcciones asignadas a dos dispositivos finales se usan como las direcciones IPv4 de origen y de destino. Durante el proceso de encapsulación, el host de origen coloca su dirección IPv4 en el encabezado del paquete unicast como la dirección de origen y la dirección IPv4 del host de destino en el encabezado del paquete como la dirección de destino. Independientemente de si el destino especificado para un paquete es unicast, broadcast o multicast, la dirección de origen de cualquier paquete es siempre la dirección unicast del host de origen.

Las direcciones de host IPv4 son direcciones unicast y se encuentran en el rango de direcciones de 0.0.0.0 a 223.255.255.255. Sin embargo, dentro de este rango existen muchas direcciones reservadas para fines específicos.

Transmisión de broadcast

El tráfico de broadcast se utiliza para enviar paquetes a todos los hosts en la red usando la dirección de broadcast para la red. Para broadcast, el paquete contiene una dirección IP de destino con todos unos (1) en la porción de host. Esto significa que todos los hosts de esa red local (dominio de broadcast) recibirán y verán el paquete. Muchos protocolos de red, como DHCP, utilizan broadcasts. Cuando un host recibe un paquete enviado a la dirección de broadcast de red, el host procesa el paquete de la misma manera en la que procesaría un paquete dirigido a su dirección unicast.

La transmisión de broadcast se usa para ubicar servicios/dispositivos especiales para los cuales no se conoce la dirección o cuando un host debe brindar información a todos los hosts de la red.

Algunos ejemplos para utilizar una transmisión de broadcast son:

- Asignar direcciones de capa superior a direcciones de capa inferior
- Solicitar una dirección.
- Intercambiar información de enrutamiento por medio de protocolos de enrutamiento
- A diferencia de unicast, donde los paquetes pueden ser enrutados por toda la internetwork, los paquetes de broadcast normalmente se restringen a la red local. Esta restricción depende de la configuración del router del gateway y del tipo de broadcast. Existen dos tipos de broadcasts: broadcast dirigido y broadcast limitado.

Cuando un host necesita información envía una solicitud, llamada consulta, a la dirección de broadcast. Todos los hosts de la red reciben y procesan esta consulta. Uno o más hosts que poseen la información solicitada responderán, típicamente mediante unicast.

De forma similar, cuando un host necesita enviar información a los hosts de una red, éste crea y envía un paquete de broadcast con la información.

Broadcast dirigido

Un broadcast dirigido se envía a todos los hosts de una red específica. Este tipo de broadcast es útil para enviar un broadcast a todos los hosts de una red local. Por ejemplo, para que un host fuera de la red 172.16.4.0/24 se comunique con todos los hosts dentro de esa red, la dirección de destino del paquete sería 172.16.4.255. Aunque los routers no reenvían broadcasts dirigidos de manera predeterminada, se les puede configurar para que lo hagan.

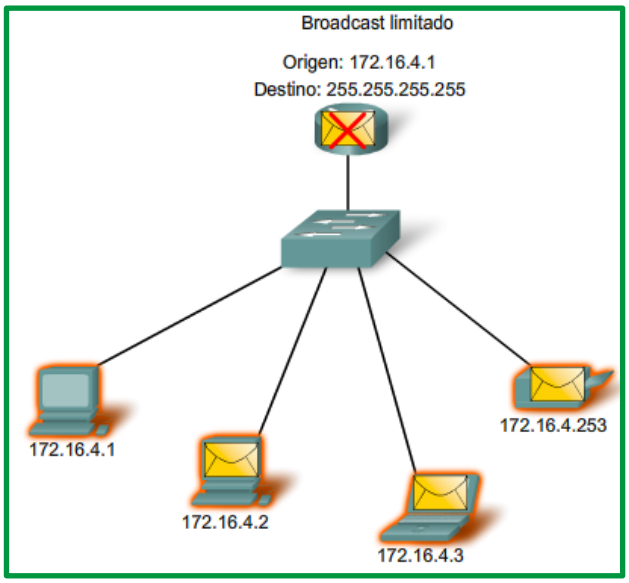


Figure 120. Broadcast limitada

Broadcast limitado

El broadcast limitado se usa para la comunicación que está limitada a los hosts en la red local. Estos paquetes siempre utilizan la dirección IPv4 de destino 255.255.255.255. Los routers no reenvían broadcasts limitados. Por esta razón, también se hace referencia a una red IPv4 como un dominio de broadcast. Los routers son dispositivos fronterizos para un dominio de broadcast.

A modo de ejemplo, un host dentro de la red 172.16.4.0/24 transmitiría a todos los hosts en su red utilizando un paquete con una dirección de destino 255.255.255.255.

Cuando se transmite un paquete, utiliza recursos en la red y hace que cada host receptor en la red procese el paquete. Por lo tanto, el tráfico de broadcast debe limitarse para que no afecte negativamente el rendimiento de la red o de los dispositivos. Debido a que los routers separan dominios de broadcast, subdividir las redes con tráfico de broadcast excesivo puede mejorar el rendimiento de la red.

Como se mostró anteriormente, cuando se transmite un paquete, éste utiliza recursos de la red y de esta manera obliga a cada host de la red que lo recibe a procesar el paquete. Por lo tanto, el tráfico de broadcast debe limitarse para que no afecte negativamente el rendimiento de la red o de los dispositivos. Debido a que los routers separan dominios de broadcast, subdividir las redes con tráfico de broadcast excesivo puede mejorar el rendimiento de la red.

Transmisión de multicast

La transmisión de multicast está diseñada para conservar el ancho de banda de las redes IPv4. Reduce el tráfico al permitir que un host envíe un único paquete a un conjunto seleccionado de hosts que forman parte de un grupo multicast suscrito. Para alcanzar hosts de destino múltiples mediante la comunicación unicast, sería necesario que el host de origen envíe un paquete individual dirigido a cada host. Con multicast, el host de origen puede enviar un único paquete que llegue a miles de hosts de destino. La responsabilidad de la internetwork es reproducir los flujos multicast en un modo eficaz para que alcancen solamente a los destinatarios.

Algunos ejemplos de transmisión de multicast son:

- Transmisiones de video y de audio
- Intercambio de información de enrutamiento por medio de protocolos de enrutamiento
- Distribución de software
- Juegos remotos
- Suministro de noticias

Direcciones multicast

IPv4 tiene un bloque de direcciones reservadas para direccionar grupos multicast. Este rango de direcciones va de 224.0.0.0 a 239.255.255.255. El rango de direcciones multicast está subdividido en distintos tipos de direcciones: direcciones de ***enlace local reservadas*** y ***direcciones agrupadas globalmente.*** Un tipo adicional de dirección multicast son las direcciones agrupadas administrativamente, también llamadas direcciones de agrupamiento limitado.

Las direcciones IPv4 multicast de 224.0.0.0 a 224.0.0.255 son direcciones de enlace local reservadas. Estas direcciones se utilizarán con grupos multicast en una red local. Un router conectado a la red local reconoce que estos paquetes están dirigidos a un grupo multicast de enlace local y nunca los reenvía nuevamente. Un uso común de las direcciones de link-local reservadas se da en los protocolos de enrutamiento usando transmisión multicast para intercambiar información de enrutamiento.

Las direcciones agrupadas globalmente son de 224.0.1.0 a 238.255.255.255. Se les puede usar para transmitir datos en Internet mediante multicast. Por ejemplo, se reservó 224.0.1.1 para que el protocolo de hora de red (NTP) sincronice los relojes con la hora del día de los dispositivos de red.

Clientes multicast

Los hosts que reciben datos multicast específicos se denominan “clientes multicast”. Los clientes multicast utilizan servicios solicitados por un programa cliente para subscribirse al grupo multicast.

Cada grupo multicast está representado por una sola dirección IPv4 de destino multicast. Cuando un host IPv4 se suscribe a un grupo multicast, el host procesa paquetes dirigidos a esta dirección multicast y paquetes dirigidos a su dirección unicast asignada exclusivamente.

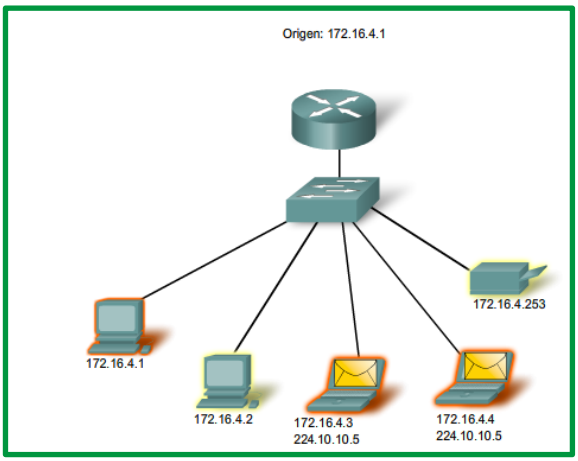


Figure 121. Trafico de multicast

TIPOS DE DIRECCIONES IPV4.

Aunque la mayoría de las direcciones IPv4 de host son direcciones públicas designadas para uso en redes a las que se accede desde Internet, existen bloques de direcciones que se utilizan en redes que requieren o no acceso limitado a Internet. Estas direcciones se denominan direcciones privadas.

Direcciones privadas

Los bloques de direcciones privadas son:

- 10.0.0.0 a 10.255.255.255 (10.0.0.0/8)
- 172.16.0.0 a 172.31.255.255 (172.16.0.0/12)
- 192.168.0.0 a 192.168.255.255 (192.168.0.0/16)

Las direcciones privadas se definen en RFC 1918, Asignación de direcciones para redes de Internet privadas, y en ocasiones se hace referencia a ellas como direcciones RFC 1918. Los bloques de direcciones de espacio privado, como se muestra en la ilustración, se utilizan en redes privadas. Los hosts que no requieren acceso a Internet pueden utilizar direcciones privadas. Sin embargo, dentro de la red privada, los hosts aún requieren direcciones IP únicas dentro del espacio privado.

Hosts en distintas redes pueden utilizar las mismas direcciones de espacio privado. Los paquetes que utilizan estas direcciones como la dirección de origen o de destino no deberían aparecer en el Internet pública. El router o el dispositivo de firewall del perímetro de estas redes privadas deben bloquear o convertir estas direcciones. Incluso si estos paquetes fueran a llegar hasta Internet, los routers no tendrían rutas para reenviarlos a la red privada correcta.

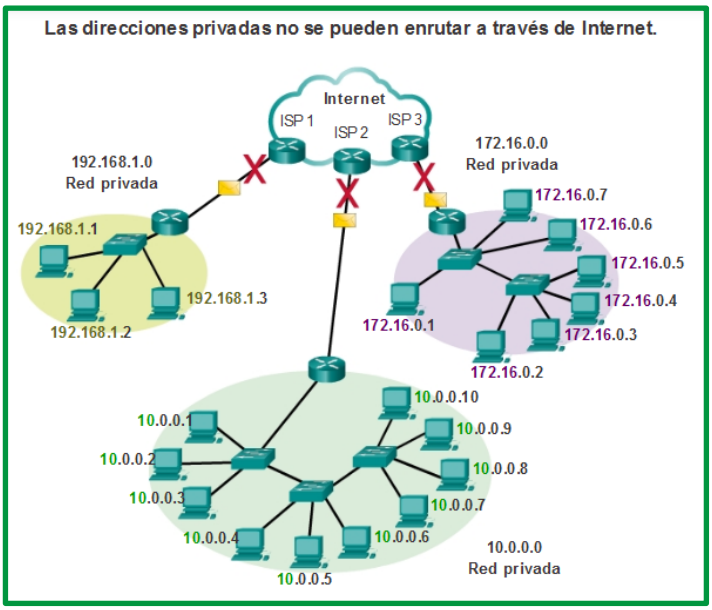


Figure 122. Direcciones IPv4 privadas

En RFC 6598, IANA reservó otro grupo de direcciones conocidas como “espacio de dirección compartido”. Como sucede con el espacio de dirección privado definido en RFC 1918, las direcciones del espacio de dirección compartido no son enrutables globalmente. Sin embargo, el propósito de estas direcciones es solamente ser utilizadas en redes de proveedores de servicios. El bloque de direcciones compartido es 100.64.0.0/10.

Traducción de direcciones de red (NAT)

Con servicios para traducir las direcciones privadas a direcciones públicas, los hosts en una red direccionada en forma privada pueden tener acceso a recursos a través de Internet. Estos servicios, llamados Traducción de dirección de red (NAT), pueden ser implementados en un dispositivo en un extremo de la red privada.

NAT permite a los hosts de la red "pedir prestada" una dirección pública para comunicarse con redes externas. A pesar de que existen algunas limitaciones y problemas de rendimiento con NAT, los clientes de la mayoría de las aplicaciones pueden acceder a los servicios de Internet sin problemas evidentes.

Direcciones públicas

La amplia mayoría de las direcciones en el rango de host unicast IPv4 son direcciones públicas. Estas direcciones están diseñadas para ser utilizadas en los hosts de acceso público desde Internet. Aun dentro de estos bloques de direcciones IPv4, existen muchas direcciones designadas para otros fines específicos.

Existen determinadas direcciones que no pueden asignarse a los hosts. También hay direcciones especiales que pueden asignarse a los hosts, pero con restricciones respecto de la forma en que dichos hosts pueden interactuar dentro de la red.

Direcciones de red y de broadcast

Como se explicó anteriormente, no es posible asignar la primera ni la última dirección a hosts dentro de cada red. Éstas son, respectivamente, la dirección de red y la dirección de broadcast.

Ruta predeterminada

También anteriormente presentada, se representa la ruta predeterminada IPv4 como 0.0.0.0. La ruta predeterminada se usa como ruta "comodín" cuando no se dispone de una ruta más específica. El uso de esta dirección también reserva todas las direcciones en el bloque de direcciones 0.0.0.0 - 0.255.255.255 (0.0.0.0 /8).

Loopback

Una de estas direcciones reservadas es la dirección de loopback IPv4 127.0.0.1. La dirección de loopback es una dirección especial que los hosts utilizan para dirigir el tráfico hacia ellos mismos. La dirección de loopback crea un método de acceso directo para las aplicaciones y servicios TCP/IP que se ejecutan en el mismo dispositivo para comunicarse entre sí. Al utilizar la dirección de loopback en lugar de la dirección host IPv4 asignada, dos servicios en el mismo host pueden desviar las capas inferiores del stack de TCP/IP. También es posible hacer ping a la dirección de loopback para probar la configuración de TCP/IP en el host local.

A pesar de que sólo se usa la dirección única 127.0.0.1, se reservan las direcciones 127.0.0.0 a 127.255.255.255. Cualquier dirección dentro de este bloque producirá un loop back al host local. Las direcciones dentro de este bloque no deben figurar en ninguna red.

Direcciones link-local

Las direcciones IPv4 del bloque de direcciones que va de 169.254.0.0 a 169.254.255.255 (169.254.0.0/16) se designan como direcciones link-local. El sistema operativo puede asignar automáticamente estas direcciones al host local en entornos donde no se dispone de una configuración IP. Se pueden utilizar en una red punto a punto pequeña o para un host que no pudo obtener una dirección de un servidor de DHCP automáticamente.

La comunicación mediante direcciones link-local IPv4 sólo es adecuada para comunicarse con otros dispositivos conectados a la misma red, como se muestra en la figura. Un host no debe enviar un paquete con una dirección de destino link-local IPv4 a ningún router para ser reenviado, y debería establecer el tiempo de vida (TLL) de IPv4 para estos paquetes en 1.

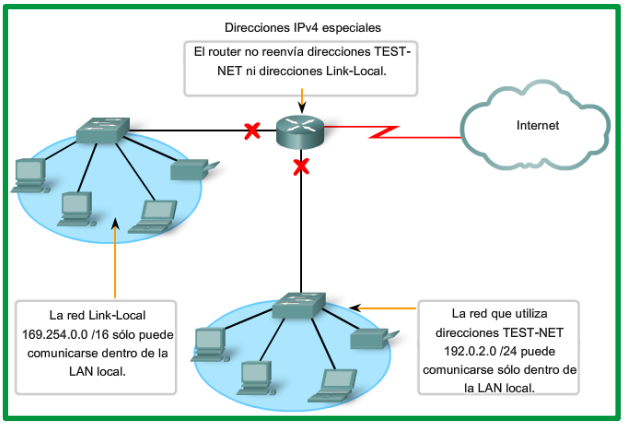


Figure 123. Direcciones IPv4 especiales

Las direcciones link-local no proporcionan servicios fuera de la red local. Sin embargo, muchas aplicaciones de cliente/servidor y punto a punto funcionarán correctamente con direcciones de enlace local IPv4.

Direcciones TEST-NET

El bloque de direcciones que va de 192.0.2.0 a 192.0.2.255 (192.0.2.0/24) se reserva para fines de enseñanza y aprendizaje. Estas direcciones pueden usarse en ejemplos de documentación y redes. A diferencia de las direcciones experimentales, los dispositivos de red aceptarán estas direcciones en su configuración. A menudo puede encontrar que estas direcciones se usan con los nombres de dominio ***example.com*** o ***example.net*** en la documentación de las RFC, del fabricante y del protocolo. Las direcciones dentro de este bloque no deben aparecer en Internet.

Direcciones experimentales

Las direcciones del bloque que va de 240.0.0.0 a 255.255.255.254 se indican como reservadas para uso futuro (RFC 3330). En la actualidad, estas direcciones solo se pueden utilizar para fines de investigación o experimentación, y no se pueden utilizar en una red IPv4. Sin embargo, según RFC 3330, podrían, técnicamente, convertirse en direcciones utilizables en el futuro.

Enlaces de interés y revisión:

Direcciones de enlace local http://www.ietf.org/rfc/rfc3927.txt?number=3927

Direcciones IPv4 de uso especial http://www.ietf.org/rfc/rfc3330.txt?number=3330

IPv4 Multicast http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xhtml

CLASE DE DIRECCIONES IP

Históricamente, RFC1700, Assigned Numbers (Números asignados), agrupaba rangos unicast en tamaños específicos llamados “direcciones de clase A, de clase B y de clase C”. También definía a las direcciones de clase D (multicast) y de clase E (experimental), anteriormente tratadas. Las direcciones unicast de clases A, B y C definían redes de tamaños específicos y bloques de direcciones específicos para estas redes. Se asignó a una compañía u organización todo un bloque de direcciones de clase A, clase B o clase C. Este uso de espacio de dirección se denomina direccionamiento con clase.

Bloques de clase A

Se diseñó un bloque de direcciones de clase A para admitir redes extremadamente grandes con más de 16 millones de direcciones host. Las direcciones IPv4 de clase A usaban un prefijo /8 fijo, donde el primer octeto indicaba la dirección de red. Los tres octetos restantes se usaban para las direcciones host. Todas las direcciones de clase A requerían que el bit más significativo del octeto de orden superior fuera un cero. Esto significaba que había solo 128 redes de clase A posibles, 0.0.0.0/8 a 127.0.0.0/8. A pesar de que las direcciones de clase A reservaban la mitad del espacio de direcciones, debido al límite de 128 redes, sólo podían ser asignadas a aproximadamente 120 compañías u organizaciones.

Bloques de clase B

El espacio de direcciones de clase B fue diseñado para admitir las necesidades de redes de tamaño moderado a grande con hasta aproximadamente 65 000 hosts. Una dirección IP de clase B usaba los dos octetos de orden superior para indicar la dirección de red. Los dos octetos restantes especificaban las direcciones host. Al igual que con la clase A, debía reservarse espacio de direcciones para las clases de direcciones restantes. Con las direcciones de clase B, los dos bits más significativos del octeto de orden superior eran 10. Esto restringía el bloque de direcciones para la clase B a 128.0.0.0/16 hasta 191.255.0.0/16. La clase B tenía una asignación de direcciones ligeramente más eficaz que la clase A, debido a que dividía equitativamente el 25% del total del espacio total de direcciones IPv4 entre alrededor de 16 000 redes.

Bloques de clase C

El espacio de direcciones de clase C era la clase de direcciones antiguas más comúnmente disponible. Este espacio de direcciones tenía el propósito de proporcionar direcciones para redes pequeñas con un máximo de 254 hosts. Los bloques de direcciones de clase C utilizaban el prefijo /24. Esto significaba que una red de clase C usaba sólo el último octeto como direcciones host, con los tres octetos de orden superior para indicar la dirección de red. Los bloques de direcciones de clase C reservaban espacio de dirección utilizando un valor fijo de 110 para los tres bits más significativos del octeto de orden superior. Esto restringía el bloque de direcciones para la clase C a 192.0.0.0/24 hasta 223.255.255.0/24. A pesar de que ocupaba solo el 12,5% del total del espacio de direcciones IPv4, podía proporcionar direcciones a dos millones de redes.

Clases de direcciones IP

Clase de dirección	Rango del 1er octeto (decimal)	Bits del primer octeto (los bits verdes no cambian)	Red (N) y Host (H) partes de la dirección	Máscara de subred predeterminada (decimal y binaria)	Cantidad de redes y hosts posibles por red
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 redes (2^7) 16 777 214 hosts por red (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16 384 redes (2^14) 65 534 hosts por red (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2 097 150 redes (2^21) 254 hosts por red (2^8-2)
D	224-239	11100000-11101111	No disponible (multicast)		
E	240-255	11110000-11111111	No disponible (experimental)		

Nota: una combinación de todos ceros (0) o de todos unos (1) constituye direcciones de host no válidas.

Figure 124. Clases de Direcciones IP

Los bloques de direcciones de clase C reservaban espacio de direcciones para la clase D (multicast) y la clase E (experimental) mediante el uso de un valor fijo de 110 para los tres bits más significativos del octeto de orden superior. Esto restringió el bloque de direcciones para la clase C de 192.0.0.0 /16 a 223.255.255.0 /16. A pesar de que ocupaba sólo el 12.5% del total del espacio de direcciones IPv4, podía suministrar direcciones a 2 millones de redes

Limitaciones del sistema basado en clases

No todos los requisitos de las organizaciones se ajustaban a una de estas tres clases. La asignación con clase de espacio de direcciones a menudo desperdiciaba muchas direcciones, lo cual agotaba la disponibilidad de direcciones IPv4. Por ejemplo: una compañía con una red con 260 hosts necesitaría que se le otorgue una dirección de clase B con más de 65.000 direcciones.

A pesar de que este sistema con clase no fue abandonado hasta finales de la década del 90, es posible ver restos de estas redes en la actualidad. Por ejemplo, cuando asigna una dirección IPv4 a una PC, el sistema operativo examina la dirección que se asigna, a fin de determinar si esta dirección es una dirección de clase A, de clase B o de clase C. A continuación, el sistema operativo supone el prefijo utilizado por esa clase y lleva a cabo la asignación de la máscara de subred predeterminada.

Otro ejemplo es la adopción de la máscara por parte de algunos protocolos de enrutamiento. Cuando algunos protocolos de enrutamiento reciben una ruta publicada, se puede adoptar la longitud del prefijo de acuerdo con la clase de dirección.

Direccionamiento de red IPv6

IPv6 está diseñado para ser el sucesor de IPv4. IPv6 tiene un mayor espacio de direcciones de 128 bits, lo que proporciona 340 sextillones de direcciones. (Eso es el número 340 seguido de 36 ceros). Sin embargo, IPv6 es mucho más que una mera dirección más extensa. Cuando el IETF comenzó el desarrollo de una sucesora de IPv4, utilizó esta oportunidad para corregir las limitaciones de IPv4 e incluir mejoras adicionales. Un ejemplo es el protocolo de mensajes de control de Internet versión 6 (ICPMv6), que incluye la resolución de direcciones y la configuración automática de direcciones, las cuales no se encuentran en ICMP para IPv4 (ICMPv4).

Necesidad de utilizar IPv6

El agotamiento del espacio de direcciones IPv4 fue el factor que motivó la migración a IPv6. Debido al aumento de la conexión a Internet en África, Asia y otras áreas del mundo, las direcciones IPv4 ya no son suficientes para admitir este crecimiento. El lunes 31 de enero de 2011, la IANA asignó los últimos dos bloques de direcciones IPv4 /8 a los registros regionales de Internet (RIR). Diversas proyecciones indican que entre 2015 y 2020 se habrán acabado las direcciones IPv4 en los cinco RIR. En ese momento, las direcciones IPv4 restantes se habrán asignado a los ISP.

IPv4 tiene un máximo teórico de 4300 millones de direcciones. Las direcciones privadas definidas en RFC 1918 junto con la traducción de direcciones de red (NAT) fueron un factor determinante para retardar el agotamiento del espacio de direcciones IPv4. La NAT tiene limitaciones que obstaculizan gravemente las comunicaciones punto a punto.

Internet de las cosas

En la actualidad, Internet es significativamente distinta de cómo era en las últimas décadas. Hoy en día, Internet es más que correo electrónico, páginas Web y transferencia de archivos entre PC. Internet evoluciona y se está convirtiendo en una ***Internet de las cosas***. Los dispositivos que acceden a Internet ya no serán solamente PC, tablet PC y smartphones. Los dispositivos del futuro preparados para acceder a Internet y equipados con sensores incluirán desde automóviles y dispositivos biomédicos hasta electrodomésticos y ecosistemas naturales. Imagine una reunión en la ubicación de un cliente que se programa en forma automática en la aplicación de calendario para que comience una hora antes de la hora en que normalmente comienza a

trabajar. Esto podría ser un problema importante, en especial si olvida revisar el calendario o ajustar el despertador según corresponda. Ahora imagine que la aplicación de calendario comunica esta información directamente al despertador para usted y su automóvil. El automóvil calienta automáticamente para derretir el hielo del limpiaparabrisas antes de que usted ingrese y cambia la ruta hacia el lugar de la reunión.

Con una creciente población de Internet, un espacio limitado de direcciones IPv4, problemas con la NAT y con Internet de las cosas, llegó el momento de iniciar la transición a IPv6.

No hay una única fecha para realizar la transición a IPv6. En un futuro cercano, IPv4 e IPv6 coexistirán. Se espera que la transición demore años. El IETF creó diversos protocolos y herramientas para ayudar a los administradores de red a migrar las redes a IPv6. Las técnicas de migración pueden dividirse en tres categorías:

- ***Dual-stack***: Como se muestra en la figura, la técnica dual-stack permite que IPv4 e IPv6 coexistan en la misma red. Los dispositivos dual-stack ejecutan stacks de protocolos IPv4 e IPv6 de manera simultánea.

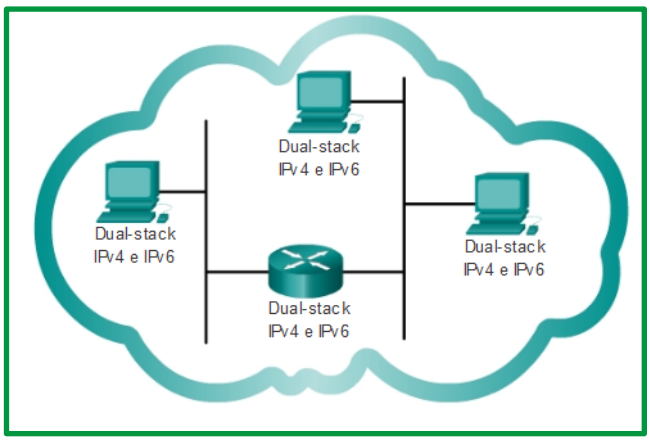


Figure 125. Dual-Stack

- ***Tunneling***: Como se muestra en la figura, tunneling es un método para transportar paquetes IPv6 a través de redes IPv4. El paquete IPv6 se encapsula dentro de un paquete IPV4, de manera similar a lo que sucede con otros tipos de datos.

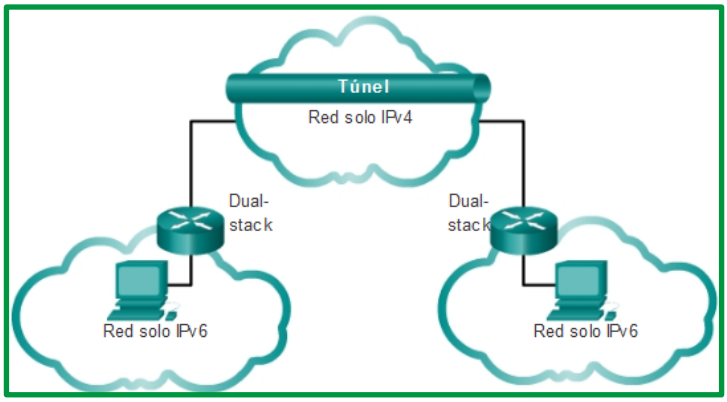


Figure 126. Tunneling

- ***Traducción***: Como se muestra en la figura, la traducción de direcciones de red 64 (NAT64) permite que los dispositivos con IPv6 habilitado se comuniquen con dispositivos con IPv4 habilitado mediante una técnica de traducción similar a la NAT para IPv4. Un paquete IPv6 se traduce en un paquete IPV4, y viceversa.

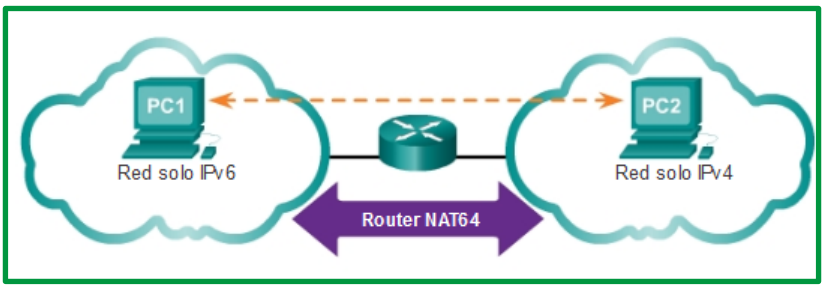


Figure 127. Traducción

Asignación de direcciones IPv6

A diferencia de las direcciones IPv4, que se expresan en notación decimal punteada, las direcciones IPv6 se representan mediante valores hexadecimales. Usted observó que el formato hexadecimal se utiliza en el panel Packets Byte (Byte del paquete) de Wireshark. En Wireshark, el formato hexadecimal se utiliza para representar los valores binarios dentro de tramas y paquetes. El formato hexadecimal también se utiliza para representar las direcciones de control de acceso al medio (MAC) de Ethernet.

Numeración hexadecimal

El método hexadecimal ("Hex") es una manera conveniente de representar valores binarios. Así como el sistema de numeración decimal es un sistema de base diez y el binario es un sistema de base dos, el sistema hexadecimal es un sistema de base dieciséis.

El sistema de numeración de base 16 utiliza los números del 0 al 9 y las letras de la A a la F. En la figura, se muestran los valores hexadecimales, binarios y decimales equivalentes. Existen 16 combinaciones únicas de cuatro bits, de 0000 a 1111. El sistema hexadecimal de16 dígitos es el sistema de numeración perfecto para utilizar, debido a que cuatro bits cualesquiera se pueden representar con un único valor hexadecimal.

Representación de valores hexadecimales		
Hexadecimal	Decimal	Binario
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
A	10	1010
B	11	1011
C	12	1100
D	13	1101
E	14	1110
F	15	1111

Figure 128. Valores hexadecimales, binarios y decimales equivalentes

Comprensión de los bytes

Dado que 8 bits (un byte) es una agrupación binaria común, los binarios 00000000 hasta 11111111 pueden representarse en valores hexadecimales como el intervalo 00 a FF. Se pueden mostrar los ceros iniciales para completar la representación de 8 bits. Por ejemplo, el valor binario 0000 1010 se muestra en valor hexadecimal como 0A.

Representación de valores hexadecimales

Recuerde que. - En lo que respecta a los caracteres del 0 al 9, es importante distinguir los valores hexadecimales de los decimales.

Por lo general, los valores hexadecimales se representan en forma de texto mediante el valor precedido por 0x (por ejemplo, 0x73) o un subíndice 16. Con menor frecuencia, pueden estar seguidos de una H, por ejemplo, 73H. Sin embargo, y debido a que el texto en subíndice no es reconocido en entornos de línea de comando o de programación, la representación técnica de un valor hexadecimal es precedida de "0x" (cero X). Por lo tanto, los ejemplos anteriores deberían mostrarse como 0x0A y 0x73, respectivamente.

Conversiones hexadecimales

Las conversiones numéricas entre valores decimales y hexadecimales son simples, pero no siempre es conveniente dividir o multiplicar por 16.

Con la práctica, es posible reconocer los patrones de bits binarios que coinciden con los valores decimales y hexadecimales. En la figura, se muestran estos patrones para valores seleccionados de 8 bits.

Conversión de octetos binarios a valores hexadecimales		
Hexadecimal	**Decimal**	**Binario**
00	0	0000 0000
01	1	0000 0001
02	2	0000 0010
03	3	0000 0011
04	4	0000 0100
05	5	0000 0101
06	6	0000 0110
07	7	0000 0111
08	8	0000 1000
0A	10	0000 1010
0F	15	0000 1111
10	16	0001 0000
20	32	0010 0000
40	64	0100 0000
80	128	1000 0000
C0	192	1100 0000
EC	202	1100 1010
F0	240	1111 0000
FF	255	1111 1111

Figure 129. Conversón de octeto binario a valores hexadecimal

Las direcciones IPv6 tienen una longitud de 128 bits y se escriben como una cadena de valores hexadecimales. Cuatro bits se representan mediante un único dígito hexadecimal, con un total de 32 valores hexadecimales. Las direcciones IPv6 no distinguen mayúsculas de minúsculas y pueden escribirse en minúscula o en mayúscula.

Formato preferido

Como se muestra en la figura, el formato preferido para escribir una dirección IPv6 es x:x:x:x:x:x:x:x, donde cada “x” consta de cuatro valores hexadecimales. Al hacer referencia a 8 bits de una dirección IPv4, utilizamos el término “octeto”. En IPv6, un “hexteto” es el término no oficial que se utiliza para referirse a un segmento de 16 bits o cuatro valores hexadecimales. Cada “x” es un único hexteto, 16 bits o cuatro dígitos hexadecimales.

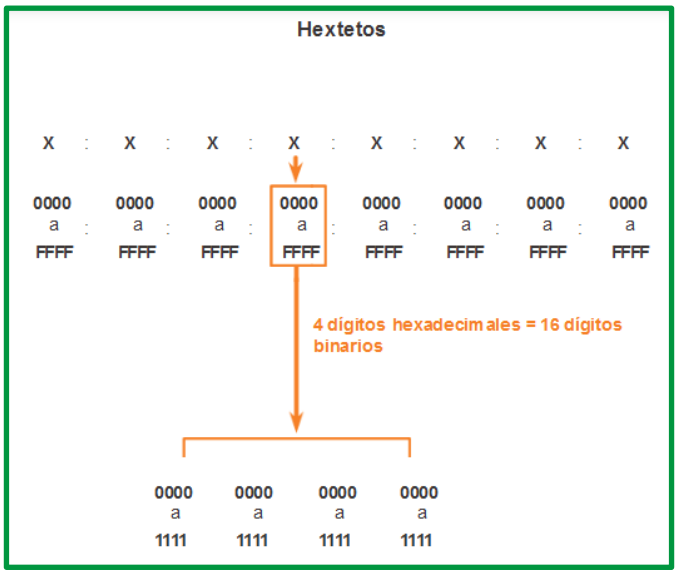


Figure 130. Hexteto

"***Formato preferido***" significa que la dirección IPv6 se escribe utilizando 32 dígitos hexadecimales. No significa necesariamente que es el método ideal para representar la dirección IPv6. En las siguientes páginas, veremos dos reglas que permiten reducir el número de dígitos necesarios para representar una dirección IPv6.

En la figura siguiente, se muestran ejemplos de direcciones IPv6 en el formato preferido.

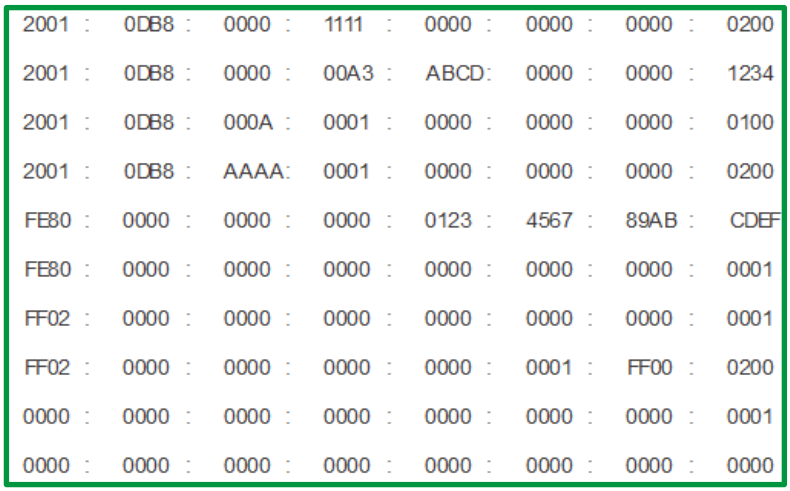


Figure 131. Formato preferido

La primera regla que permite reducir la notación de direcciones IPv6 es que se puede omitir cualquier 0 (cero) inicial en cualquier sección de 16 bits o hexteto. Por ejemplo:

- 01AB puede representarse como 1AB.
- 09F0 puede representarse como 9F0.
- 0A00 puede representarse como A00.
- 00AB puede representarse como AB.

Esta regla solo es válida para los ceros iniciales, y NO para los ceros finales; de lo contrario, la dirección sería ambigua. Por ejemplo, el hexteto "ABC" podría ser tanto "0ABC" como "ABC0".

En las siguientes ilustraciones, se muestran varios ejemplos de cómo se puede utilizar la omisión de ceros iniciales para reducir el tamaño de una dirección IPv6. Se muestra el formato preferido para cada ejemplo. Advierta cómo la omisión de ceros iniciales en la mayoría de los ejemplos da como resultado una representación más pequeña de la dirección.

Recomendado	2001:0DB8:0000:1111:0000:0000:0000:0200
Sin 0 inicial	2001:DB8:0:1111:0:0:0:200
Recomendado	2001:0DB8:0000:A300:ABCD:0000:0000:1234
Sin 0 inicial	2001:DB8:0:A300:ABCD:0:0:1234
Recomendado	2001:0DB8:000A:1000:0000:0000:0000:0100
Sin 0 inicial	2001:DB8:A:1000:0:0:0:100
Recomendado	FE80:0000:0000:0000:0123:4567:89AB:CDEF
Sin 0 inicial	FE80:0:0:0:123:4567:89AB:CDEF
Recomendado	FF02:0000:0000:0000:0000:0000:0000:0001
Sin 0 inicial	FF02:0:0:0:0:0:0:1
Recomendado	FF02:0000:0000:0000:0000:0001:FF00:0200
Sin 0 inicial	FF02:0:0:0:0:1:FF00:200
Recomendado	0000:0000:0000:0000:0000:0000:0000:0001
Sin 0 inicial	0:0:0:0:0:0:0:1
Recomendado	0000:0000:0000:0000:0000:0000:0000:0000
Sin 0 inicial	0:0:0:0:0:0:0:0

Figure 132. Ejemplos de cómo se puede utilizar la omisión de ceros iniciales

La segunda regla que permite reducir la notación de direcciones IPv6 es que los dos puntos dobles (::) pueden reemplazar cualquier cadena única y contigua de uno o más segmentos de 16 bits (hextetos) compuestos solo por ceros.

Los dos puntos dobles (::) se pueden utilizar solamente una vez dentro de una dirección; de lo contrario, habría más de una dirección resultante posible. Cuando se utiliza junto con la técnica de omisión de ceros iniciales, la notación de direcciones IPv6 generalmente se puede reducir de manera considerable. Esto se suele conocer como "***formato comprimido***".

Dirección incorrecta:

- 2001:0DB8::ABCD::1234

Expansiones posibles de direcciones comprimidas ambiguas:

- 2001:0DB8::ABCD:0000:0000:1234
- 2001:0DB8::ABCD:0000:0000:0000:1234
- 2001:0DB8:0000:ABCD::1234
- 2001:0DB8:0000:0000:ABCD::1234

En las siguientes ilustraciones, se muestran varios ejemplos de cómo el uso de los dos puntos dobles (::) y la omisión de ceros iniciales puede reducir el tamaño de una dirección IPv6.

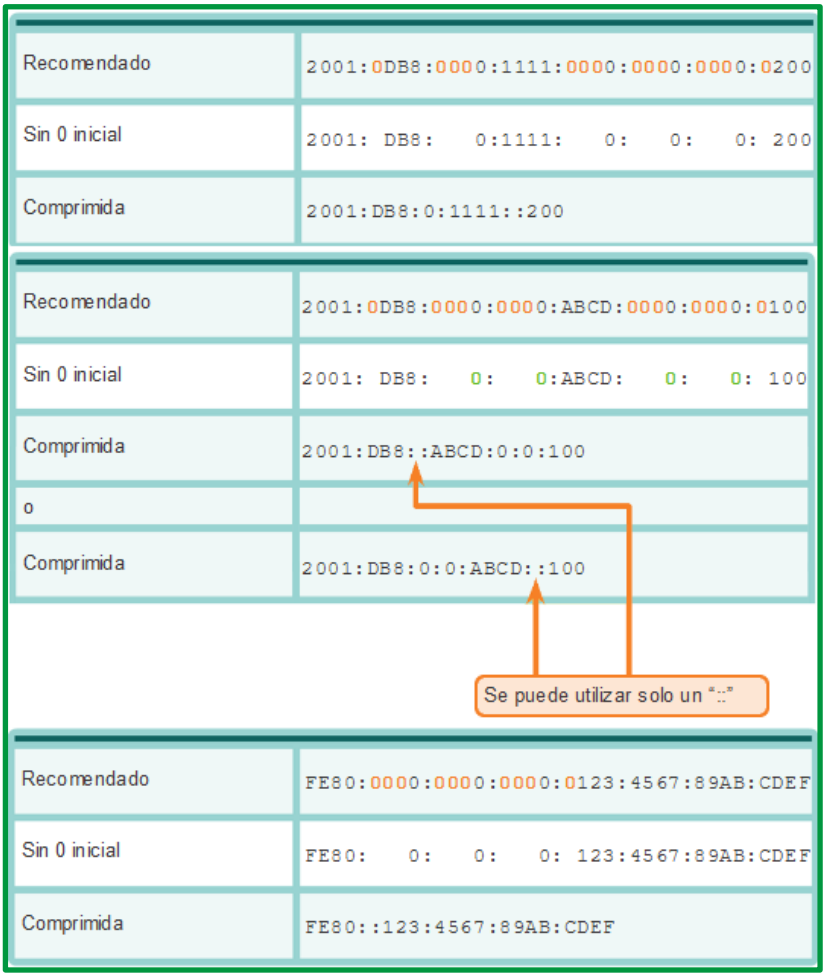


Figure 133. Ejemplos de cómo se puede utilizar :: formato comprimido en IPv6

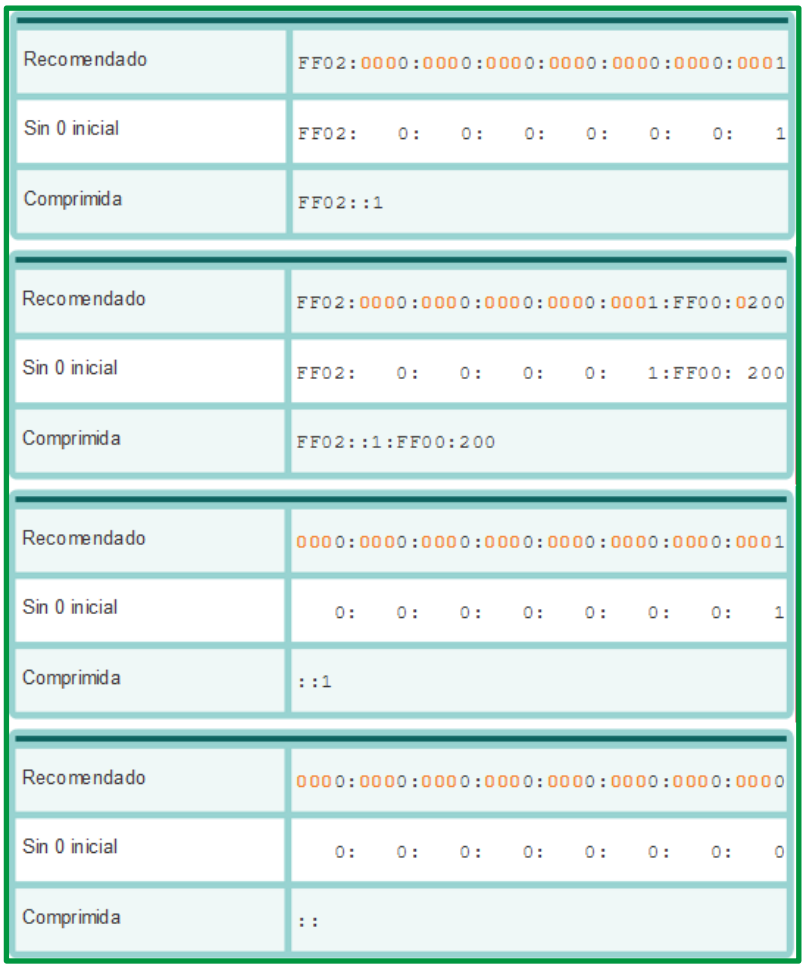


Figure 134. Figure 129. Ejemplos de cómo se puede utilizar :: formato comprimido en IPv6

Caso práctico para desarrollo del estudiante.

- *Omita los ceros iniciales*
- *Aplicar formato comprimido*

Ejercicio 1: *Convierta la dirección Ipv6 2001:0000:0DB8:1111:0000:0000:0200*

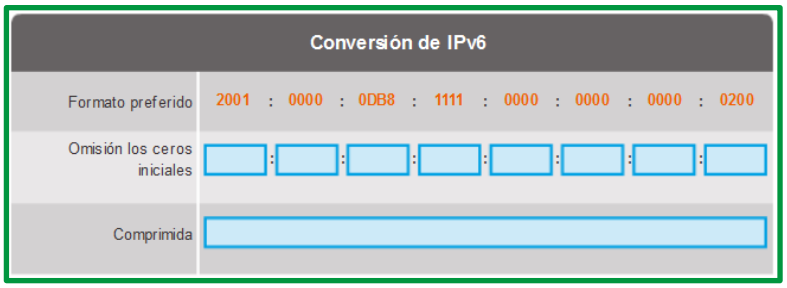


Figure 135. Caso práctico de reducción de notación IPv6

Ejercicio 2: *Convierta la dirección Ipv6 2013:0000:0123:4567:89AB:0000:CDEF:0001*

Ejercicio 3: *Convierta la dirección Ipv6 0000:0000:0000:0000:0000:0000:0000:0001*

Ejercicio 4: *Convierta la dirección Ipv6 2012:ABCD:EF01:2345:0678:0910:AAAA:BBBB*

Ejercicio 5: *Convierta la dirección Ipv6 AB1E:2B00:0000:1234:5678:9101:1112:1113*

Ejercicio 6: *Convierta la dirección Ipv6 BB2B:EF12:BFF3:9125:1111:0101:1111:0101*

Ejercicio 7: *Convierta la dirección Ipv6 1129:1984:2233:4455:6677:0000:0000:0101*

Ejercicio 8: *Convierta la dirección Ipv6 1111:0000:0000:0000:0000:0000:0101:1111*

Ejercicio 9: *Convierta la dirección Ipv6 1031:1976:0001:0001:0003:0004:0000:0101*

Ejercicio 10: *Convierta la dirección Ipv6 0000:0000:0000:1234:6678:9101:0000:34AB*

Existen tres tipos de direcciones IPv6:

- ***Unicast***: Las direcciones IPv6 unicast identifican de forma exclusiva una interfaz en un dispositivo con IPv6 habilitado. Como se muestra en la ilustración, las direcciones IPv6 de origen deben ser direcciones unicast.
- ***Multicast***: Las direcciones IPv6 multicast se utilizan para enviar un único paquete IPv6 a varios destinos.
- ***Anycast***: Las direcciones IPv6 anycast son direcciones IPv6 unicast que se pueden asignar a varios dispositivos. Los paquetes enviados a una dirección anycast se enrutan al dispositivo más cercano que tenga esa dirección. En este curso, no se analizan las direcciones anycast.

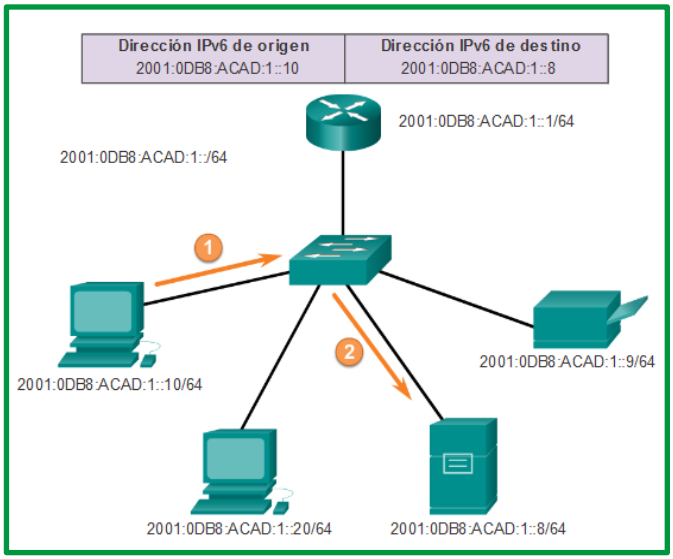


Figure 136. Comunicaciones IPv6 unicast

A diferencia de IPv4, IPv6 no tiene una dirección de broadcast. Sin embargo, existe una dirección IPv6 multicast de todos los nodos que brinda básicamente el mismo resultado.

Recuerde que es posible identificar el prefijo, o la porción de red, de una dirección IPv4 mediante una máscara de subred en formato decimal punteado o una duración de prefijo (notación con barras). Por ejemplo, la dirección IP 192.168.1.10 con la máscara de subred decimal punteada 255.255.255.0 equivale a 192.168.1.10/24.

IPv6 utiliza la duración de prefijo para representar la porción de prefijo de la dirección. IPv6 no utiliza la notación decimal punteada de máscara de subred. La duración de prefijo se utiliza para

indicar la porción de red de una dirección IPv6 mediante el formato de dirección IPv6/duración de prefijo.

La duración de prefijo puede ir de 0 a 128. Una duración de prefijo IPv6 típica para LAN y la mayoría de los demás tipos de redes es /64. Esto significa que la porción de prefijo o de red de la dirección tiene una longitud de 64 bits, lo cual deja otros 64 bits para la ID de interfaz (porción de host) de la dirección.

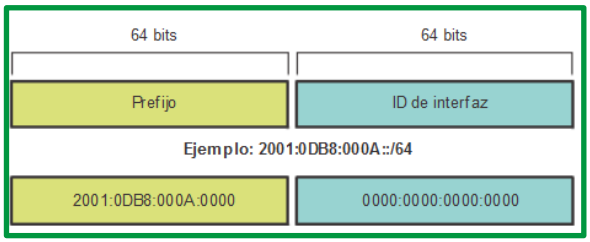


Figure 137. Ejemplo de prefijo de red Ipv6

Las direcciones IPv6 unicast identifican de forma exclusiva una interfaz en un dispositivo con IPv6 habilitado. Un paquete que se envía a una dirección unicast es recibido por la interfaz que tiene asignada esa dirección. Como sucede con IPv4, las direcciones IPv6 de origen deben ser direcciones unicast. Las direcciones IPv6 de destino pueden ser direcciones unicast o multicast.

Existen seis tipos de direcciones IPv6 unicast.

- ***Unicast global.*** Las direcciones unicast globales son similares a las direcciones IPv4 públicas. Estas son direcciones enrutables de Internet globalmente exclusivas. Las direcciones unicast globales pueden configurarse estáticamente o asignarse de forma dinámica. Existen algunas diferencias importantes con respecto a la forma en que un dispositivo recibe su dirección IPv6 dinámicamente en comparación con DHCP para IPv4.
- ***Link-local.*** Las direcciones link-local se utilizan para comunicarse con otros dispositivos en el mismo enlace local. Con IPv6, el término “enlace” hace referencia a una subred. Las direcciones link-local se limitan a un único enlace. Su exclusividad se debe confirmar solo para ese enlace, ya que no se pueden enrutar más allá del enlace. En otras palabras, los routers no reenvían paquetes con una dirección de origen o de destino link-local.
- ***Loopback.*** Los hosts utilizan la dirección de loopback para enviarse paquetes a sí mismos, y esta dirección no se puede asignar a una interfaz física. Al igual que en el caso de una dirección IPv4 de loopback, se puede hacer ping a una dirección IPv6 de loopback para probar la configuración de TCP/IP en el host local. La dirección IPv6 de loopback está formada por todos ceros, excepto el último bit, representado como ::1/128 o, simplemente, ::1 en el formato comprimido.
- ***Dirección sin especificar***. Una dirección sin especificar es una dirección compuesta solo por ceros representada como ::/128 o, simplemente, :: en formato comprimido. No puede asignarse a una interfaz y solo se utiliza como dirección de origen en un paquete IPv6. Las direcciones sin especificar se utilizan como direcciones de origen cuando el dispositivo aún no tiene una dirección IPv6 permanente o cuando el origen del paquete es irrelevante para el destino.

- ***Local única***. Las direcciones IPv6 locales únicas tienen cierta similitud con las direcciones privadas para IPv4 definidas en RFC 1918, pero también existen diferencias importantes. Las direcciones locales únicas se utilizan para el direccionamiento local dentro de un sitio o entre una cantidad limitada de sitios. Estas direcciones no deben ser enrutables en la IPv6 global. Las direcciones locales únicas están en el rango de FC00::/7 a FDFF::/7.

  Con IPv4, las direcciones privadas se combinan con NAT/PAT para proporcionar una traducción de varios a uno de direcciones privadas a públicas. Esto se hace debido a la disponibilidad limitada de espacio de direcciones IPv4. Muchos sitios también utilizan la naturaleza privada de las direcciones definidas en RFC 1918 para ayudar a proteger u ocultar su red de posibles riesgos de seguridad. Sin embargo, este nunca fue el uso que se pretendió dar a estas tecnologías, y el IETF siempre recomendó que los sitios tomen las precauciones de seguridad adecuadas en el router con conexión a Internet. Si bien IPv6 proporciona direccionamiento de sitio específico, no tiene por propósito ser utilizado para contribuir a ocultar dispositivos internos con IPv6 habilitado de Internet IPv6. El IETF recomienda que la limitación del acceso a los dispositivos se logre implementando medidas de seguridad adecuadas y recomendadas.

  En la especificación IPv6 original, se definían las direcciones locales de sitio con un propósito similar y se utilizaba el rango de prefijos FEC0::/10. La especificación contenía varias ambigüedades, y el IETF dejó en desuso las direcciones locales de sitio en favor de direcciones locales únicas.

  IPv4 integrada. El último tipo de dirección unicast es la dirección IPv4 integrada. Estas direcciones se utilizan para facilitar la transición de IPv4 a IPv6. En este curso, no se analizan las direcciones IPv4 integradas.

  Las direcciones IPv6 unicast globales son globalmente únicas y enrutables en Internet IPv6. Estas direcciones son equivalentes a las direcciones IPv4 públicas. La Internet Corporation for Assigned Names and Numbers (ICANN), el operador de la Internet Assigned Numbers Authority (IANA), asigna bloques de direcciones IPv6 a los cinco RIR. Actualmente, solo se asignan direcciones unicast globales con los tres primeros bits de 001 o 2000::/3. Esto solo constituye un octavo del espacio total disponible de direcciones IPv6, sin incluir solamente una parte muy pequeña para otros tipos de direcciones unicast y multicast.

  La dirección 2001:0DB8::/32 se reservó para fines de documentación, incluido el uso en ejemplos.

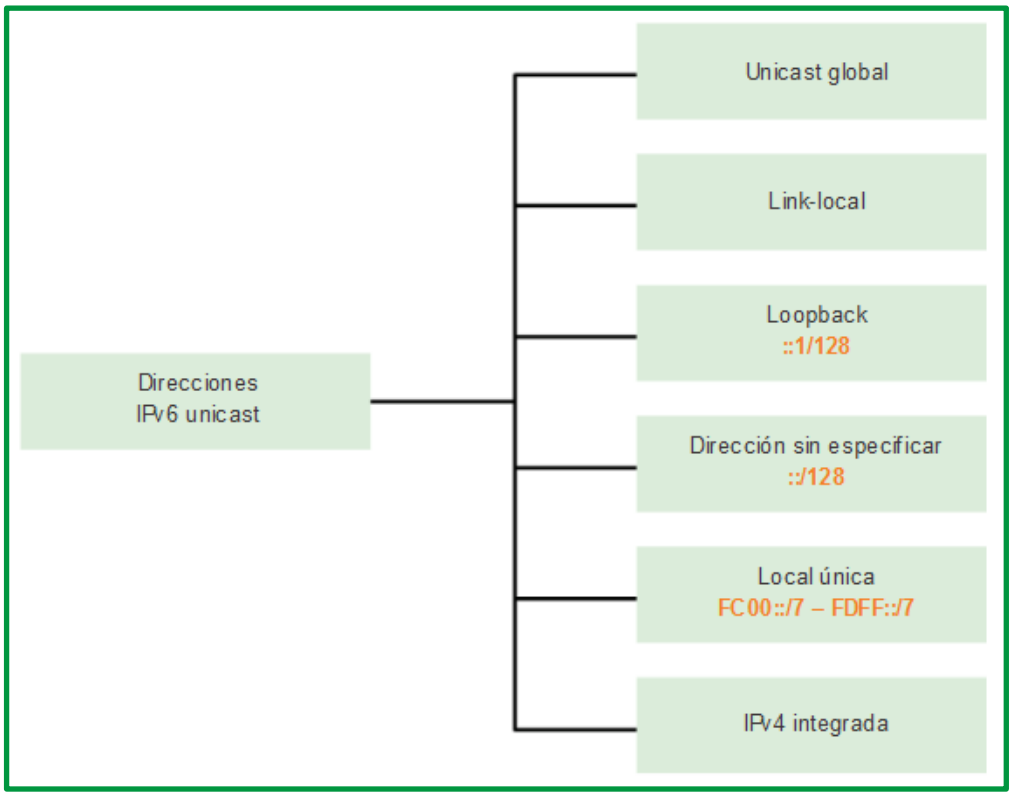


Figure 138. Direcciones IPv6 unicast

Una dirección IPv6 link-local permite que un dispositivo se comunique con otros dispositivos con IPv6 habilitado en el mismo enlace y solo en ese enlace (subred). Los paquetes con una dirección link-local de origen o de destino no se pueden enrutar más allá del enlace en el cual se originó el paquete.

A diferencia de las direcciones IPv4 link-local, las direcciones IPv6 link-local cumplen una función importante en diversos aspectos de la red. La dirección unicast global no constituye un requisito, pero toda interfaz de red con IPv6 habilitado debe tener una dirección link-local.

Si en una interfaz no se configura una dirección link-local de forma manual, el dispositivo crea automáticamente su propia dirección sin comunicarse con un servidor de DHCP. Los hosts con IPv6 habilitado crean una dirección IPv6 link-local incluso si no se asignó una dirección IPv6 unicast global al dispositivo. Esto permite que los dispositivos con IPv6 habilitado se comuniquen con otros dispositivos con IPv6 habilitado en la misma subred. Esto incluye la comunicación con el gateway predeterminado (router).

Las direcciones IPv6 link-local están en el rango de FE80::/10. /10 indica que los primeros 10 bits son 1111 1110 10xx xxxx. El primer hexteto tiene un rango de 1111 1110 1000 0000 (FE80) a 1111 1110 1011 1111 (FEBF).

En la figura siguiente, se muestra un ejemplo de comunicación mediante direcciones IPv6 link-local.

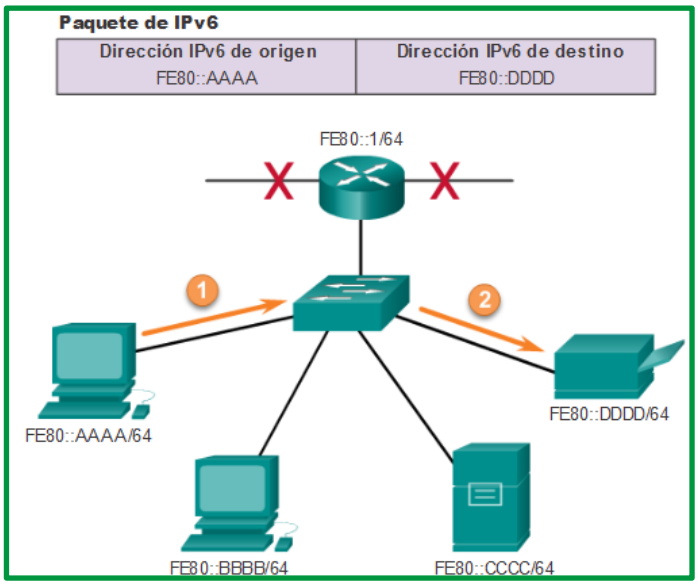


Figure 139. Comunicaciones de enlace de IPv6

En la figura siguiente, se muestra el formato de una dirección IPv6 link-local.

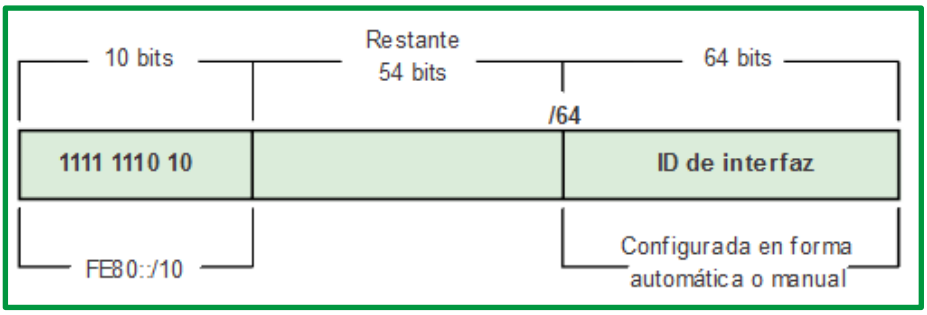


Figure 140. Dirección IPv6 link-local

Los protocolos de enrutamiento IPv6 también utilizan direcciones IPv6 link-local para intercambiar mensajes y como la dirección del siguiente salto en la tabla de enrutamiento IPv6. Las direcciones link-local se analizan más detalladamente en un curso posterior.

Nota: Por lo general, la dirección que se utiliza como gateway predeterminado para los otros dispositivos en el enlace es la dirección link-local del router, y no la dirección unicast global.

Las direcciones IPv6 unicast globales son globalmente únicas y enrutables en Internet IPv6. Estas direcciones son equivalentes a las direcciones IPv4 públicas. La Internet Corporation for Assigned Names and Numbers (ICANN), el operador de la Internet Assigned Numbers Authority (IANA), asigna bloques de direcciones IPv6 a los cinco RIR. Actualmente, solo se asignan direcciones unicast globales con los tres primeros bits de 001 o 2000::/3. Esto solo constituye un octavo del espacio total disponible de direcciones IPv6, sin incluir solamente una parte muy pequeña para otros tipos de direcciones unicast y multicast.

Nota: la dirección 2001:0DB8::/32 se reservó para fines de documentación, incluido el uso en ejemplos.

Figure 141. Estructura y el rango de una dirección unicast global

Una dirección unicast global consta de tres partes:

- Prefijo de enrutamiento global
- ID de subred
- ID de interfaz

Prefijo de enrutamiento global

El prefijo de enrutamiento global es la porción de prefijo, o de red, de la dirección que asigna el proveedor (por ejemplo, un ISP) a un cliente o a un sitio. En la actualidad, los RIR asignan a los clientes el prefijo de enrutamiento global /48. Esto incluye desde redes comerciales de empresas hasta unidades domésticas Para la mayoría de los clientes, este espacio de dirección es más que suficiente.

En la figura siguiente, se muestra la estructura de una dirección unicast global con el prefijo de enrutamiento global /48. Los prefijos /48 son los prefijos de enrutamiento global más comunes, y se utilizarán en la mayoría de los ejemplos a lo largo de este curso.

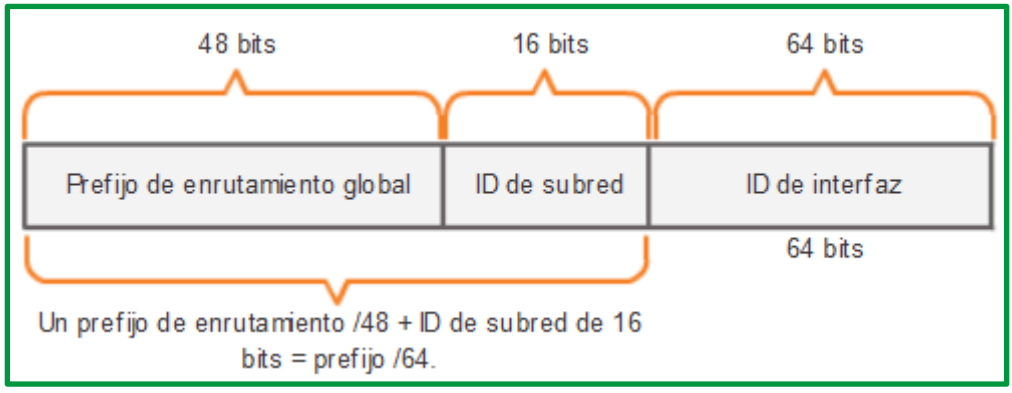


Figure 142. prefijo de enrutamiento global /48 de IPv6

Por ejemplo, la dirección IPv6 2001:0DB8:ACAD::/48 tiene un prefijo que indica que los primeros 48 bits (3 hextetos) (2001:0DB8:ACAD) son la porción de prefijo o de red de la dirección. Los dos puntos dobles (::) antes de la duración de prefijo /48 significan que el resto de la dirección se compone solo de ceros.

ID de subred

Las organizaciones utilizan la ID de subred para identificar una subred dentro de su ubicación.

ID de interfaz

La ID de interfaz IPv6 equivale a la porción de host de una dirección IPv4. Se utiliza el término "ID de interfaz" debido a que un único host puede tener varias interfaces, cada una con una o más direcciones IPv6.

A diferencia de IPv4, en IPv6 se pueden asignar las direcciones de host compuestas solo por ceros y unos a un dispositivo. Se puede usar la dirección compuesta solo por unos debido al hecho de que en IPv6 no se usan las direcciones de broadcast. También se puede utilizar la dirección compuesta solo por ceros, pero se reserva como una dirección anycast de subred y router, y se debe asignar solo a routers.

Una forma fácil de leer la mayoría de las direcciones IPv6 es contar la cantidad de hextetos. Como se muestra en la figura siguiente, en una dirección unicast global /64 los primeros cuatro hextetos son para la porción de red de la dirección, y el cuarto hexteto indica la ID de subred. Los cuatro hextetos restantes son para la ID de interfaz.

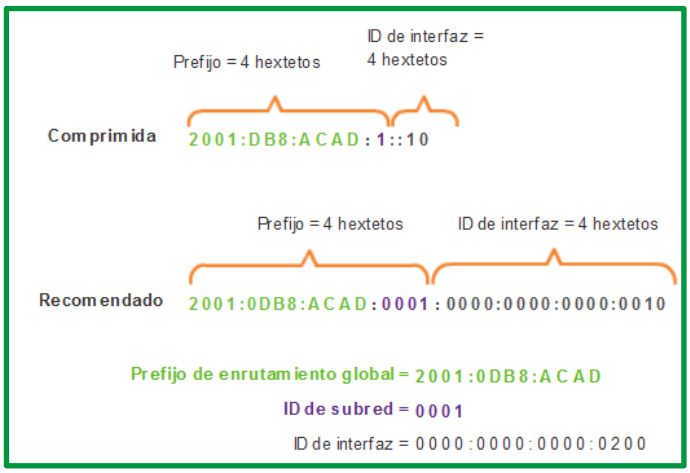


Figure 143. Lectura de una dirección unicast global

Proceso EUI-64

El IEEE definió el identificador único extendido (EUI) o proceso EUI-64 modificado. Este proceso utiliza la dirección MAC de Ethernet de 48 bits de un cliente e introduce otros 16 bits en medio de la dirección MAC de 48 bits para crear una ID de interfaz de 64 bits.

Las direcciones MAC de Ethernet, por lo general, se representan en formato hexadecimal y constan de dos partes:

- Identificador único de organización (OUI): el OUI es un código de proveedor de 24 bits (seis dígitos hexadecimales) que asigna el IEEE.
- Identificador de dispositivo: el identificador de dispositivo es un valor único de 24 bits (seis dígitos hexadecimales) dentro de un OUI común.

Las ID de interfaz EUI-64 se representan en sistema binario y constan de tres partes:

- OUI de 24 bits de la dirección MAC del cliente, pero el séptimo bit (bit universal/local, U/L) se invierte. Esto significa que, si el séptimo bit es un 0, se convierte en 1, y viceversa.

- Valor de 16 bits FFFE introducido (en formato hexadecimal)
- Identificador de dispositivo de 24 bits de la dirección MAC del cliente

En la figura siguiente, se ilustra el proceso EUI-64, con la siguiente dirección MAC de GigabitEthernet de R1: FC99:4775:CEE0.

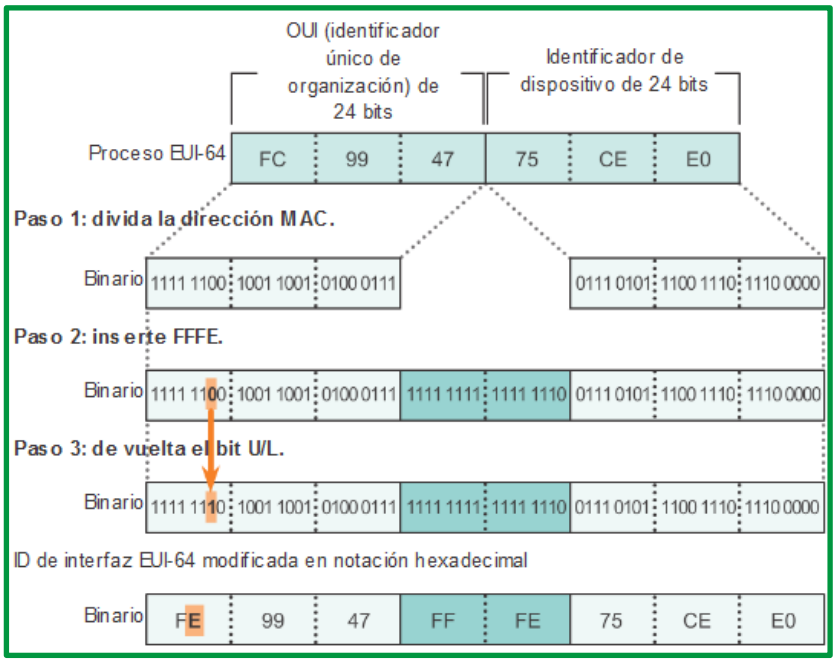


Figure 144. Proceso EUI-64

Paso 1: Dividir la dirección MAC entre el OUI y el identificador de dispositivo

Paso 2: Insertar el valor hexadecimal FFFE, que en formato binario es: 1111 1111 1111 1110

Paso 3: Convertir los primeros dos valores hexadecimales del OUI a binario e invertir el bit U/L (séptimo bit) En este ejemplo, el 0 en el bit 7 se cambia a 1.

El resultado es una ID de interfaz de FE99:47FF:FE75:CEE0 generada mediante EUI-64.

El uso del bit U/L y los motivos para invertir su valor se analizan en RFC 5342.

La ventaja de EUI-64 es que se puede utilizar la dirección MAC de Ethernet para determinar la ID de interfaz. También permite que los administradores de red rastreen fácilmente una dirección IPv6 a un dispositivo final mediante la dirección MAC única. Sin embargo, esto generó inquietudes con respecto a la privacidad a muchos usuarios. Les preocupa que los paquetes puedan ser rastreados a la PC física real. Debido a estas inquietudes, se puede utilizar en cambio una ID de interfaz generada aleatoriamente.

ID de interfaz generadas aleatoriamente

Según el sistema operativo, un dispositivo puede utilizar una ID de interfaz generada aleatoriamente en lugar de utilizar la dirección MAC y el proceso EUI-64. Por ejemplo, comenzando con Windows Vista, Windows utiliza una ID de interfaz generada aleatoriamente en lugar de una ID de interfaz creada mediante EUI-64. Windows XP y sistemas operativos Windows anteriores utilizaban EUI-64.

Una manera sencilla de identificar que una dirección muy probablemente se creó mediante EUI-64 es el valor FFFE ubicado en medio de la ID de interfaz, como se muestra en la figura siguiente.

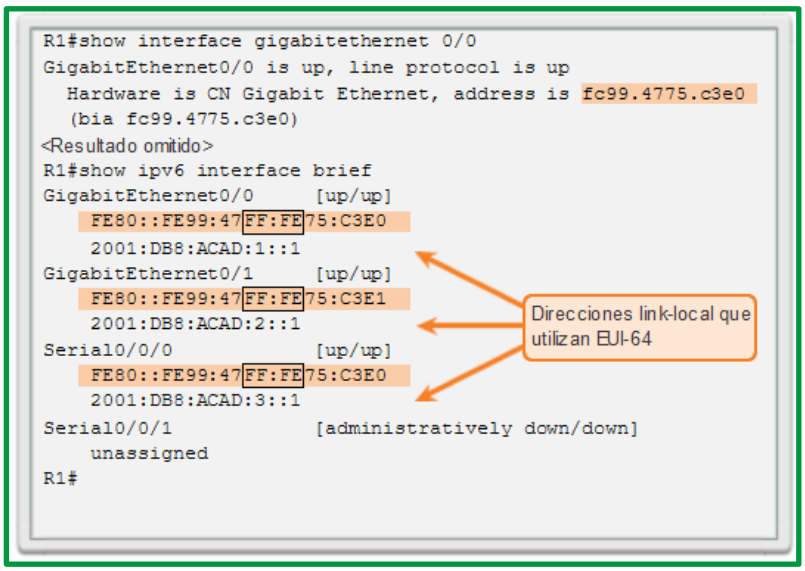


Figure 145. Direcciones link-local que utiliza EUI-64

Después de que se establece una ID de interfaz, ya sea mediante el proceso EUI-64 o mediante la generación aleatoria, se puede combinar con un prefijo IPv6 para crear una dirección unicast global o una dirección link-local.

- ***Dirección unicast global***: Al utilizar SLAAC, el dispositivo recibe su prefijo del mensaje de RA de ICMPv6 y lo combina con la ID de interfaz.
- ***Dirección link-local***: Los prefijos link-local comienzan con FE80::/10. Los dispositivos suelen utilizar FE80::/64 como prefijo o duración de prefijo, seguido de la ID de interfaz.

Al utilizar SLAAC (SLAAC solamente o SLAAC con DHCPV6), los dispositivos reciben el prefijo y la duración de prefijo del mensaje de RA de ICMPv6. Debido a que el mensaje de RA designa el prefijo de la dirección, el dispositivo debe proporcionar únicamente la porción de ID de interfaz de su dirección. Como se indicó anteriormente, la ID de interfaz se puede generar de forma automática mediante el proceso EUI-64, o, según el OS, se puede generar de forma aleatoria. Con la información del mensaje de RA y la ID de interfaz, el dispositivo puede establecer su dirección unicast global.

Después de que se asigna una dirección unicast global a una interfaz, el dispositivo con IPv6 habilitado genera la dirección link-local automáticamente. Los dispositivos con IPv6 habilitado deben tener, como mínimo, la dirección link-local. Recuerde que una dirección IPv6 link-local permite que un dispositivo se comunique con otros dispositivos con IPv6 habilitado en la misma subred.

Las direcciones IPv6 link-local se utilizan para diversos fines, incluidos los siguientes:

- Los hosts utilizan la dirección link-local del router local para obtener la dirección IPv6 de gateway predeterminado.
- Los routers intercambian mensajes de protocolo de enrutamiento dinámico mediante direcciones link-local.

- Las tablas de enrutamiento de los routers utilizan la dirección link-local para identificar el router del siguiente salto al reenviar paquetes IPv6.

Las direcciones link-local se pueden establecer dinámicamente o se pueden configurar de forma manual como direcciones link-local estáticas.

Dirección link-local asignada dinámicamente

La dirección link-local se crea dinámicamente mediante el prefijo FE80::/10 y la ID de interfaz.

De manera predeterminada, los routers en los que se utiliza Cisco IOS utilizan EUI-64 para generar la ID de interfaz para todas las direcciones link-local en las interfaces IPv6. Para las interfaces seriales, el router utiliza la dirección MAC de una interfaz Ethernet. Recuerde que una dirección link-local debe ser única solo en ese enlace o red. Sin embargo, una desventaja de utilizar direcciones link-local asignadas dinámicamente es su longitud, que dificulta identificar y recordar las direcciones asignadas.

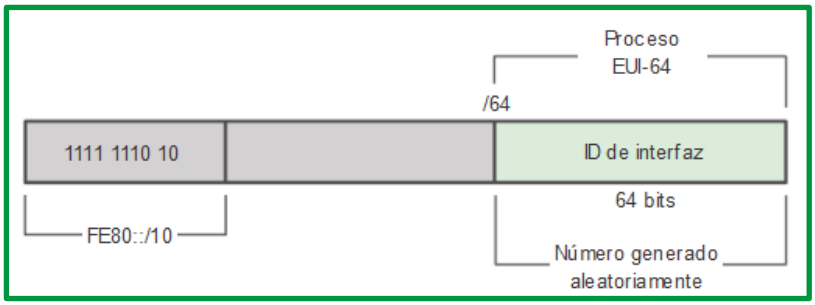


Figure 146. Dirección IPv6 link-local

Dirección Link-Local estática

Configurar la dirección link-local de forma manual permite crear una dirección reconocible y más fácil de recordar.

Las direcciones link-local pueden configurarse manualmente mediante el mismo comando interface que se utiliza para crear direcciones IPv6 unicast globales, pero con un parámetro adicional:

Router(config-if)#ipv6 address link-local-address link-local

En la figura siguiente, se muestra que una dirección link-local tiene un prefijo dentro del rango FE80 a FEBF. Cuando una dirección comienza con este hexteto (segmento de 16 bits), el parámetro link-local debe seguir la dirección.

```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address fe80::1 ?
  link-local  Use link-local address

R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#
```

Figure 147. Configuración de direcciones link-local en el R1

En la figura siguiente, se muestra la configuración de una dirección link-local mediante el comando ipv6 address interface. La dirección link-local FE80::1 se utiliza para que sea posible reconocer fácilmente que pertenece al router R1. Se configura la misma dirección IPv6 link-local en todas las interfaces de R1. Se puede configurar FE80::1 en cada enlace, debido a que solamente tiene que ser única en ese enlace.

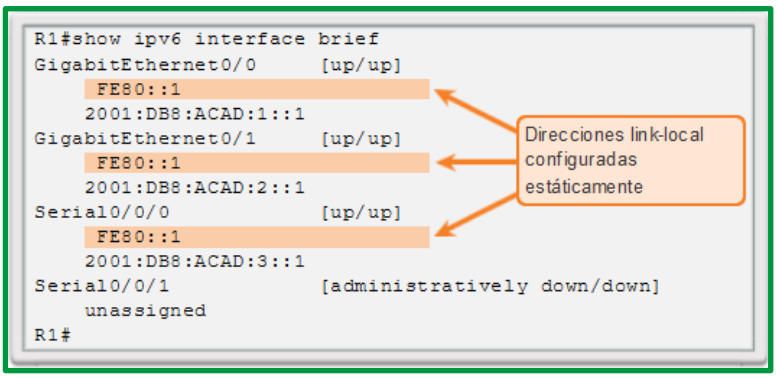


Figure 148. Configuración de una dirección link-local en R1

De manera similar a R1, el router R2 se configuraría con FE80::2 como la dirección IPv6 link-local en todas sus interfaces.

Direcciones IPv6 multicast.

Las direcciones IPv6 multicast son similares a las direcciones IPv4 multicast. Recuerde que las direcciones multicast se utilizan para enviar un único paquete a uno o más destinos (grupo multicast). Las direcciones IPv6 multicast tienen el prefijo FF00::/8. Las direcciones multicast solo pueden ser direcciones de destino, no de origen.

Existen dos tipos de direcciones IPv6 multicast:

- Dirección multicast asignada
- Dirección multicast de nodo solicitado

Dirección multicast asignada

Las direcciones multicast asignadas son direcciones multicast reservadas para grupos predefinidos de dispositivos. Una dirección multicast asignada es una única dirección que se utiliza para llegar a un grupo de dispositivos que ejecutan un protocolo o servicio común. Las

direcciones multicast asignadas se utilizan en contexto con protocolos específicos, como DHCPv6.

Dos grupos comunes de direcciones multicast IPv6 asignadas incluyen los siguientes:

Grupo multicast de todos los nodos FF02::1: grupo multicast al que se unen todos los dispositivos con IPv6 habilitado. Los paquetes que se envían a este grupo son recibidos y procesados por todas las interfaces IPv6 en el enlace o en la red. Esto tiene el mismo efecto que una dirección de broadcast en IPv4. En la ilustración, se muestra un ejemplo de comunicación mediante la dirección multicast de todos los nodos. Un router IPv6 envía mensajes de RA de protocolo de mensajes de control de Internet versión 6 (ICMPv6) al grupo multicast de todos los nodos. El mensaje de RA proporciona a todos los dispositivos en la red con IPv6 habilitado la información de direccionamiento, como el prefijo, la duración de prefijo y el gateway predeterminado.

Grupo multicast de todos los routers FF02::2: grupo multicast al que se unen todos los routers con IPv6 habilitado. Un router se convierte en un miembro de este grupo cuando se habilita como router IPv6 mediante el comando de configuración global ipv6 unicast-routing. Los paquetes que se envían a este grupo son recibidos y procesados por todos los routers IPv6 en el enlace o en la red.

Los dispositivos con IPv6 habilitado envían mensajes de solicitud de router (RS) de ICMPv6 a la dirección multicast de todos los routers. El mensaje de RS solicita un mensaje de RA del router IPv6 para contribuir a la configuración de direcciones del dispositivo.

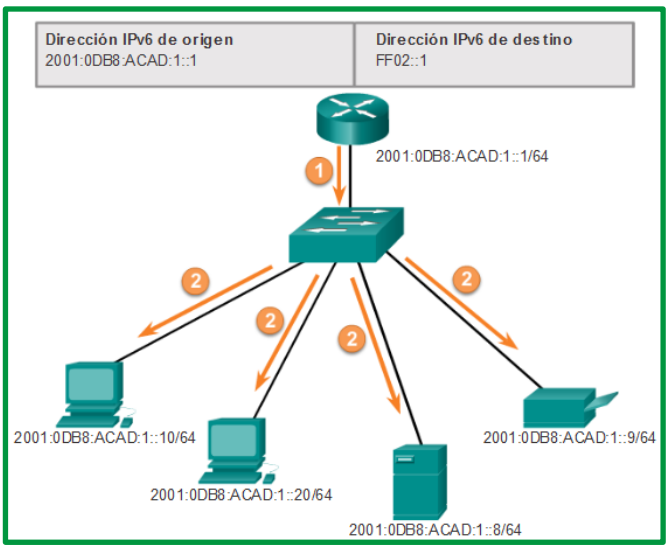


Figure 149. Comunicaciones IPv6 multicast de todos los nodos

Las direcciones multicast de nodo solicitado son similares a las direcciones multicast de todos los nodos. Recuerde que la dirección multicast de todos los nodos es esencialmente lo mismo que una dirección IPv4 de broadcast. Todos los dispositivos en la red deben procesar el tráfico enviado a la dirección de todos los nodos. Para reducir el número de dispositivos que deben procesar tráfico, utilice una dirección multicast de nodo solicitado.

Una dirección multicast de nodo solicitado es una dirección que coincide solo con los últimos 24 bits de la dirección IPv6 unicast global de un dispositivo. Los únicos dispositivos que deben procesar estos paquetes son aquellos que tienen estos mismos 24 bits en la porción menos significativa que se encuentra más hacia la derecha de la ID de interfaz.

Una dirección IPv6 multicast de nodo solicitado se crea de forma automática cuando se asigna la dirección unicast global o la dirección unicast link-local. La dirección IPv6 multicast de nodo solicitado se crea combinando un prefijo especial FF02:0:0:0:0:1:FF00::/104 con los 24 bits de su dirección unicast que se encuentran en el extremo derecho.

La dirección multicast de nodo solicitado consta de dos partes:

- ***Prefijo multicast FF02:0:0:0:0:1:FF00::/104*:** los primeros 104 bits de la dirección multicast de todos los nodos solicitados.
- ***24 bits menos significativos*:** Los 24 bits finales o que se encuentran más hacia la derecha de la dirección multicast de nodo solicitado. Estos bits se copian de los 24 bits del extremo derecho de la dirección unicast global o unicast link-local del dispositivo**.**

Es posible que varios dispositivos tengan la misma dirección multicast de nodo solicitado. Si bien es poco común, esto puede suceder cuando los dispositivos tienen los mismos 24 bits que se encuentran más hacia la derecha en sus ID de interfaz. Esto no genera ningún problema, ya que el dispositivo aún procesa el mensaje encapsulado, el cual incluye la dirección IPv6 completa del dispositivo en cuestión.

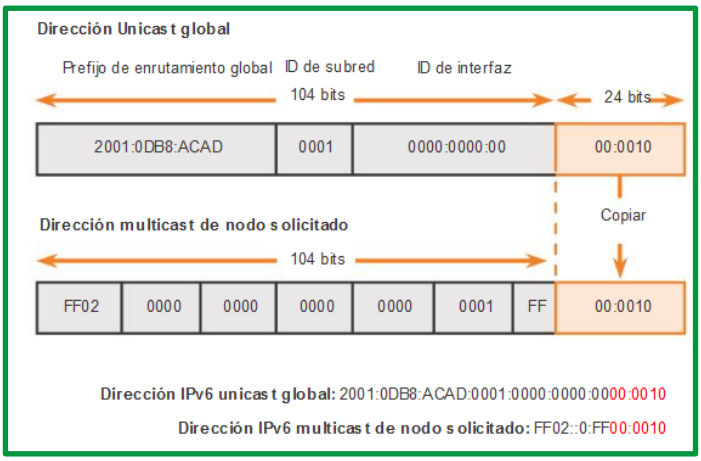


Figure 150. Dirección IPv6 multicast de nodo solicitado

Cálculo de direcciones (Subredes y sumarización)

Direccionamiento con clase

En las primeras redes IP se utilizaba lo que se denomina direccionamiento con clases, que se introdujo en 1981 como parte de la definición del protocolo IP en el [RFC 791], distinguiéndose distintas clases de direcciones. Las clases se establecen en base a los primeros bits de la dirección Las direcciones de clases A, B y C están dedicadas al direccionamiento de hosts.

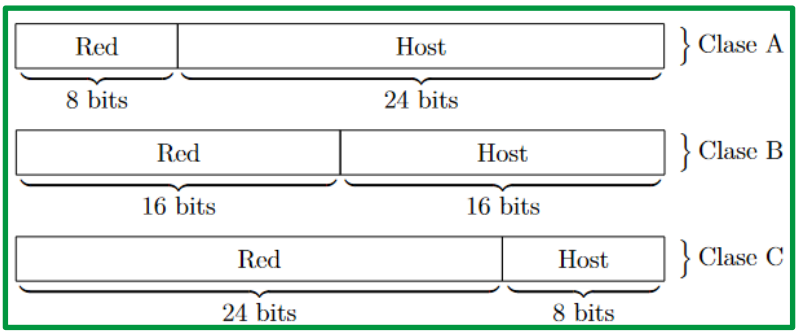


Figure 151. Prefijos de red de la clase A, B, C

En la especificación original de IPv4, los autores establecieron las clases para proporcionar tres tamaños distintos de redes para organizaciones grandes, medianas y pequeñas. Por consiguiente, se definieron las direcciones de clase A, B y C con un formato específico para los bits de orden superior. Los bits de orden superior son los bits del extremo izquierdo en una dirección de 32 bits.

Clase	Bits de orden superior	Inicio	Finalizar
Clase A	0xxxxxxx	0.0.0.0	127.255.255.255
Clase B	10xxxxxx	128.0.0.0	191.255.255.255
Clase C	110xxxxx	192.0.0.0	223.255.255.255
Clase D (multidifusión)	1110xxxx	224.0.0.0	239.255.255.255
Clase E (reservada)	1111xxxx	240.0.0.0	255.255.255.255

Figure 152. Bit de orden superior

Como se muestra en la figura:

- Direcciones de clase A que comienzan con 0: diseñadas para organizaciones grandes. Esta clase incluye todas las direcciones de 0.0.0.0 (00000000) a 127.255.255.255 (01111111). La dirección 0.0.0.0 se reserva para el routing predeterminado y la dirección 127.0.0.0, para la prueba de loopback.
- Direcciones de clase B que comienzan con 10: diseñadas para organizaciones medianas a grandes. Esta clase incluye todas las direcciones de 128.0.0.0 (10000000) a 191.255.255.255 (10111111).
- Direcciones de clase C que comienzan con 110: diseñadas para organizaciones pequeñas a medianas. Esta clase incluye todas las direcciones de 192.0.0.0 (11000000) a 223.255.255.255 (11011111).

Las direcciones restantes se reservaron para multicasting y futuros usos.

Direcciones de multidifusión de clase D que comienzan con 1110: las direcciones de multidifusión se utilizan para identificar un grupo de hosts que forman parte de un grupo de multidifusión. Esto ayuda a reducir la cantidad de procesamientos de paquetes que realizan los hosts, en especial en los medios de difusión (es decir, las LAN Ethernet). Los protocolos de routing, como RIPv2, EIGRP y OSPF, utilizan direcciones de multidifusión designadas (RIP = 224.0.0.9, EIGRP = 224.0.0.10, OSPF 224.0.0.5 y 224.0.0.6).

Direcciones IP de clase E reservadas que comienzan con 1111: estas direcciones se reservaron para uso experimental y futuro.

Como se especifica en RFC 790, cada clase de red tiene asociada una máscara de subred predeterminada.

Como se muestra en la figura siguiente, las redes de clase A utilizan el primer octeto para identificar la porción de red de la dirección. Esto se traduce a una máscara de subred con clase 255.0.0.0. Debido a que solo se dejaron 7 bits en el primer octeto (recuerde que el primer bit es siempre 0), se elevó el 2 a la 7.a potencia, o se generaron 128 redes. El número real es de 126 redes, porque hay dos direcciones reservadas de clase A (es decir, 0.0.0.0/8 y 127.0.0.0/8). Con 24 bits en la porción de host, cada dirección de clase A tenía capacidad para más de 16 millones de direcciones host individuales.

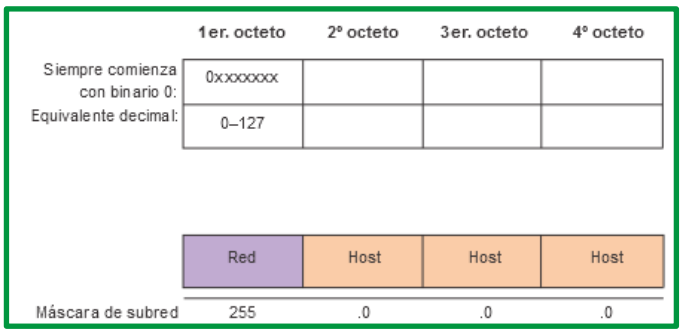


Figure 153. Redes de clase A

Como se muestra en la figura siguiente, las redes de clase B utilizan los dos primeros octetos para identificar la porción de red de la dirección de red. Con los primeros dos bits ya establecidos en 1 y 0, quedaban 14 bits en los primeros dos octetos para asignar redes, lo que produjo 16 384 direcciones de red de clase B. Debido a que cada dirección de red de clase B contenía 16 bits en la porción de host, controlaba 65 534 direcciones. (Recuerde que dos direcciones se reservaron para las direcciones de red y de difusión).

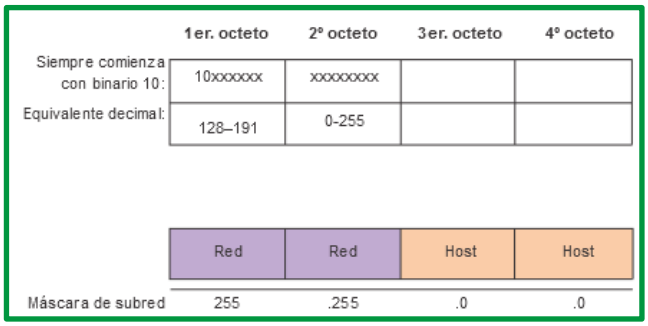


Figure 154. Redes Clase B

Como se muestra en la figura siguiente, las redes de clase C utilizan los dos primeros octetos para identificar la porción de red de la dirección de red. Con los primeros tres bits establecidos en 1 y 1, y 0, quedaban 21 bits para asignar redes para más de 2 millones de redes de clase C. Pero cada red de clase C sólo tenía 8 bits en la porción de host o 254 direcciones host posibles.

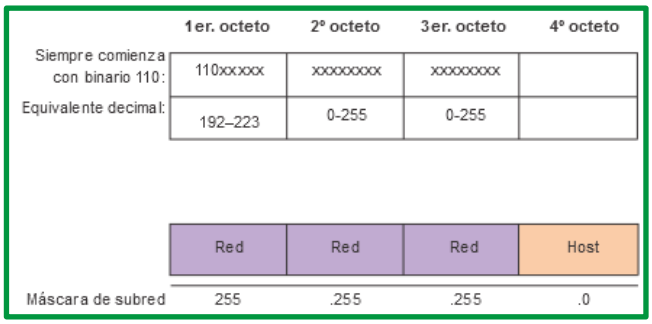


Figure 155. Redes clase C

Una ventaja de asignar máscaras de subred predeterminadas específicas a cada clase es que reduce los mensajes de actualización de routing. Los protocolos de routing con clase no incluyen la información de la máscara de subred en las actualizaciones. El router receptor aplica la máscara predeterminada según el valor del primer octeto que identifica la clase.

El resultado general fue que el direccionamiento con clase era un esquema de direccionamiento que generaba mucho desperdicio. Debía desarrollarse una mejor solución para el direccionamiento de red. Por este motivo, en 1993, se introdujo el routing entre dominios sin clase (CIDR).

Subredes.

Una vez que se asigna un prefijo principal a una organización, está por necesidades de la topología física, tendrá que subdividir la red principal en redes de menor tamaño (subredes). Esta subdivisión inicialmente se hacía alargando el prefijo de modo que la dirección IP se dividía en tres partes (Red, subred y host).

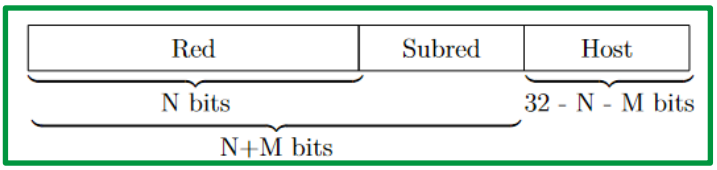


Figure 156. Prefijo y parte de host de la ip

Como se puede analizar en la figura anterior, los N primeros bits corresponden a la red, luego este prefijo de N bits se aumenta hasta N+ bits que dan lugar a los prefijos de la subred quedando finalmente 32-N-M bits para la parte de host. Para crea subredes se le quita algunos bits a la parte de host de la red original.

Inicialmente, en el [RFC 950] se consideró que las subredes debían ser todas del mismo tamaño, es decir, que la forma de hacer subredes era “robando” el número de bits suficiente de la parte de host original para indexar todas las subredes.

Ejemplo:

La división en subredes permite crear múltiples redes lógicas de un solo bloque de direcciones. Como usamos un router para conectar estas redes, cada interfaz en un router debe tener un ID único de red. Cada nodo en ese enlace está en la misma red.

Creamos las subredes utilizando uno o más de los bits del host como bits de la red. Esto se hace ampliando la máscara para tomar prestado algunos de los bits de la porción de host de la dirección, a fin de crear bits de red adicionales. Cuanto más bit de host se usen, mayor será la cantidad de subredes que puedan definirse. Para cada bit que se tomó prestado, se duplica la cantidad de subredes disponibles. Por ejemplo: si se toma prestado 1 bit, es posible definir 2 subredes. Si se toman prestados 2 bits, es posible tener 4 subredes. Sin embargo, con cada bit que se toma prestado, se dispone de menos direcciones host por subred.

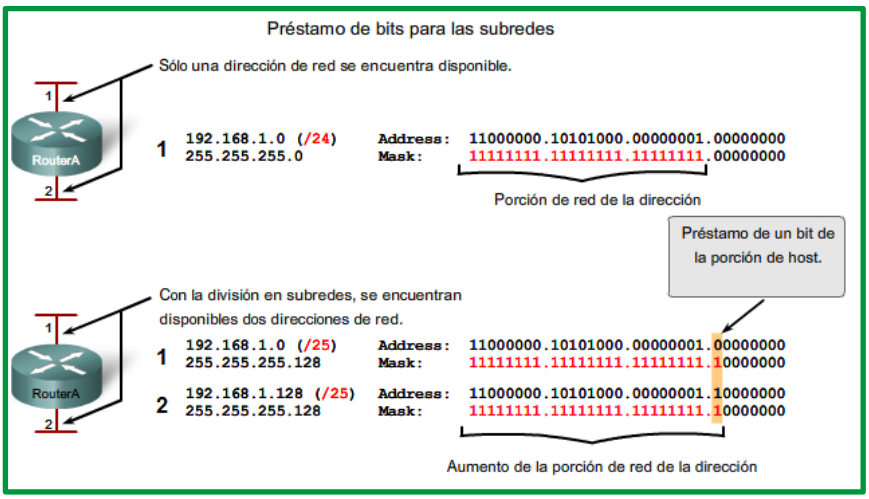


Figure 157. Subredes

El router A en la figura posee dos interfaces para interconectar dos redes. Dado un bloque de direcciones 192.168.1.0 /24, se crearán dos subredes. Se toma prestado un bit de la porción de host utilizando una máscara de subred 255.255.255.128, en lugar de la máscara original 255.255.255.0. El bit más significativo del último octeto se usa para diferenciar dos subredes. Para una de las subredes, este bit es "0" y para la otra subred, este bit es "1".

Vamos a considerar el ejemplo de clase C, teniendo claro que lo que expliquemos va a ser útil para cualquier tipo de red, sea de clase A, B o C.

Tenemos nuestra red, con dirección IP **192.168.1.0**, por lo que tenemos para asignar a los hosts de la misma todas las direcciones IP del rango **192.168.1.1** al **192.168.1.254**, ya que la dirección **192.168.1.0** será la de la propia red y la **192.168.1.255** será la dirección de broadcast general.

Si expresamos nuestra dirección de red en binario tendremos:

210.25.2.0 => 11000000.01000100.000000001.**00000000**

Con lo que tenemos 24 bits para identificar la red (en azul) y 8 bits para identificar los host (en rojo).

La máscara de red será: 255.255.255.0 => 11111111.11111111.11111111.00000000

Para crear subredes a partir de una dirección IP de red padre, la idea es "robar" bits a los hosts, pasándolos a los de identificación de red. ¿Cuántos hay bits hay que "robar"?

Depende de las subredes que queramos obtener, teniendo en cuenta que cuántas más bits robemos, más subredes obtendremos, pero con menos host cada una. Por lo tanto, el número de bits a robar depende de las necesidades de funcionamiento de la red final.

Crear 2 subredes a partir de una red Clase C. Recuerde que no siempre los valores son exactos, en este caso el resultado será 16. Según la formula 2^n debemos tomar 4 bits del rango de host, por lo tanto:

Numero de subredes => $\mathbf{2}^1=2$

Fórmula para calcular subredes

Use esta fórmula para calcular la cantidad de subredes:
2^n
donde n = la cantidad de bits que se tomaron prestados
En este ejemplo, el cálculo es así:
2^1 = 2 subredes

La cantidad de hosts

Para calcular la cantidad de hosts por red, se usa la fórmula ***2^n - 2*** donde n = la cantidad de bits para hosts.

La aplicación de esta fórmula, (2^7 - 2 = 126) muestra que cada una de estas subredes puede tener 126 hosts.

En cada subred, examine el último octeto binario. Los valores de estos octetos para las dos redes son:

Subred 1: 00000000 = 0

Subred 2: 10000000 = 128

Vea la figura para conocer el esquema de direccionamiento para estas redes.

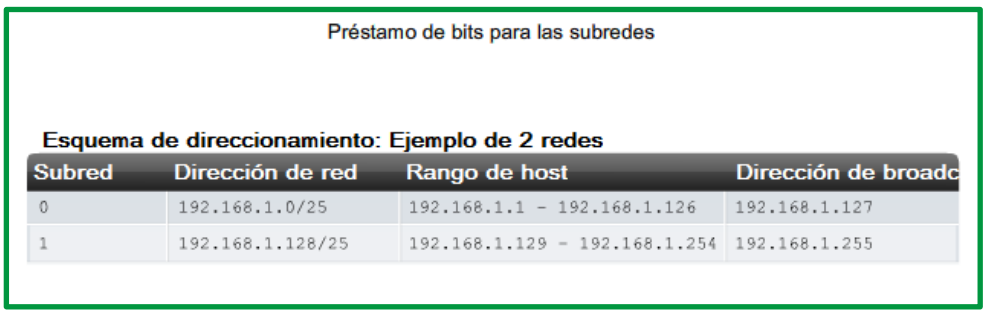


Figure 158. Esquema de direccionamiento

Ejemplo con 3 subredes

A continuación, piense en una internetwork que requiere tres subredes. Vea la figura.

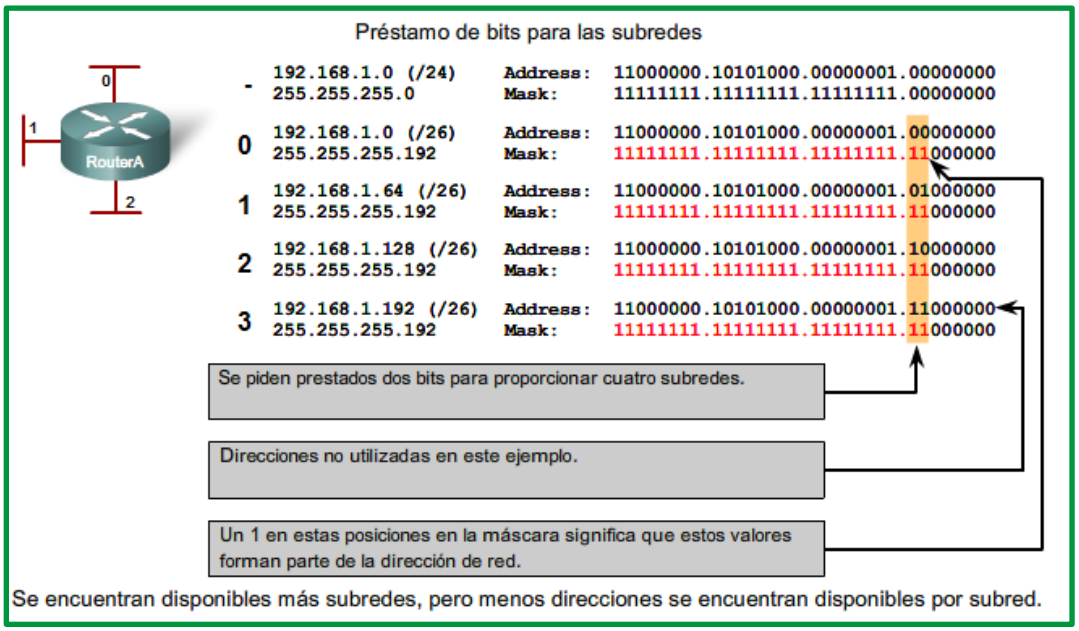


Figure 159. Ejemplo con tres subredes

Nuevamente, se comienza con el mismo bloque de direcciones 192.168.1.0 /24. Tomar prestado un solo bit proporcionará únicamente dos subredes. Para proveer más redes, se cambia la máscara de subred a 255.255.255.192 y se toman prestados dos bits. Esto proveerá cuatro subredes.

Calcule la subred con esta fórmula:

2^2 = 4 subredes

Cantidad de hosts

Para calcular la cantidad de hosts, comience por examinar el último octeto. Observe estas subredes.

Subred 0: 0 = 00000000
Subred 1: 64 = 01000000
Subred 2: 128 = 10000000
Subred 3: 192 = 11000000

Aplique la fórmula de cálculo de host.

2^6 - 2 = 62 hosts por subred

Observe la figura del esquema de direccionamiento para estas redes.

Esquema de direccionamiento: Ejemplo de 4 redes

Subred	Dirección de red	Rango de host	Dirección de broadc
0	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 - 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129 - 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 - 192.168.1.254	192.168.1.255

Figure 160. Esquema de direccionamiento de 4 redes

Ejemplo con 6 subredes

Considere este ejemplo con cinco LAN y una WAN para un total de 6 redes. Observe la figura.

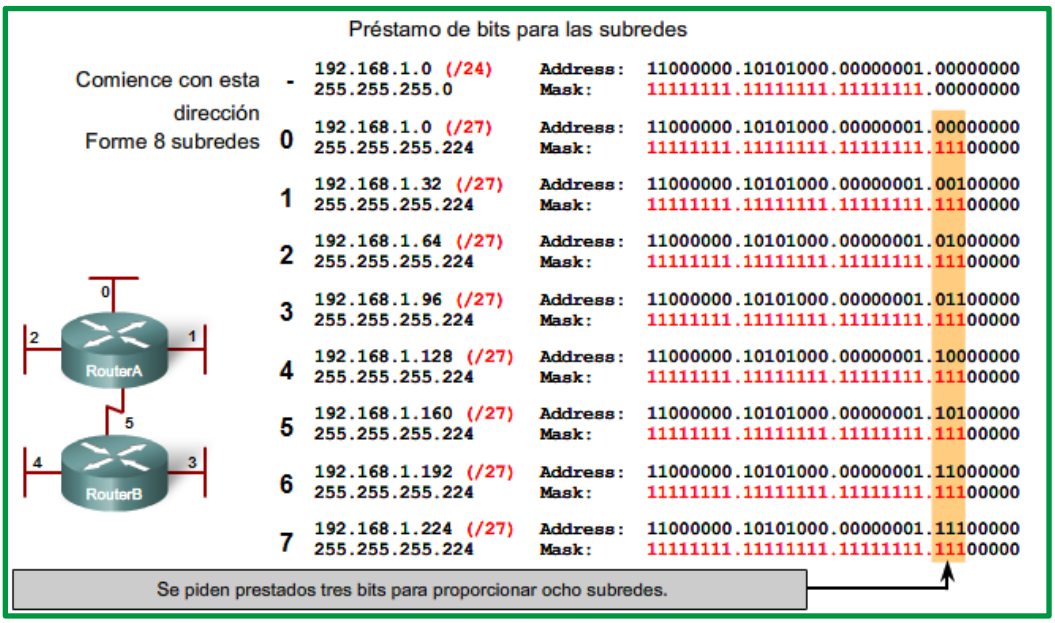


Figure 161. Ejemplo con seis subredes

Para incluir 6 redes, coloque la subred 192.168.1.0 /24 en bloques de direcciones mediante la fórmula:

2^3 = 8

Para obtener al menos 6 subredes, pida prestados tres bits de host. Una máscara de subred 255.255.255.224 proporciona los tres bits de red adicionales.

Cantidad de hosts

Para calcular la cantidad de hosts, comience por examinar el último octeto. Observe estas subredes.

0 = 00000000
32 = 00100000
64 = 01000000
96 = 01100000
128 = 10000000

160 = 10100000
192 = 11000000
224 = 11100000

Aplique la fórmula de cálculo de host:

2^5 - 2 = 30 hosts por subred.

Observe la figura del esquema de direccionamiento para estas redes.

Esquema de direccionamiento: Ejemplo de 6 redes

Subred	Dirección de red	Rango de host	Dirección de broadc
0	192.168.1.0/27	192.168.1.1 - 192.168.1.30	192.168.1.31
1	192.168.1.32/27	192.168.1.33 - 192.168.1.62	192.168.1.63
2	192.168.1.64/27	192.168.1.65 - 192.168.1.94	192.168.1.95
3	192.168.1.96/27	192.168.1.97 - 192.168.1.126	192.168.1.127
4	192.168.1.128/27	192.168.1.129 - 192.168.1.158	192.168.1.159
5	192.168.1.160/27	192.168.1.161 - 192.168.1.190	192.168.1.191
6	192.168.1.192/27	192.168.1.193 - 192.168.1.222	192.168.1.223
7	192.168.1.224/27	192.168.1.225 - 192.168.1.254	192.168.1.255

Figure 162. Esquema de direccionamiento de 8 subredes

DIVISIÓN EN SUBREDES

Cada red dentro de la internetwork de una empresa u organización está diseñada para incluir una cantidad limitada de hosts.

Algunas redes, como enlaces WAN punto a punto, sólo requieren un máximo de dos hosts. Otras redes, como una LAN de usuario en un edificio o departamento grande, pueden necesitar la inclusión de cientos de hosts. Es necesario que los administradores de red diseñen el esquema de direccionamiento de la internetwork para incluir la cantidad máxima de hosts para cada red. La cantidad de hosts en cada división debe permitir el crecimiento de la cantidad de hosts.

Determine la cantidad total de hosts

Primero, considere la cantidad total de hosts necesarios por toda la internetwork corporativa. Se debe usar un bloque de direcciones lo suficientemente amplio como para incluir todos los dispositivos en todas las redes corporativas. Esto incluye dispositivos de usuarios finales, servidores, dispositivos intermediarios e interfaces de routers.

Paso 1.

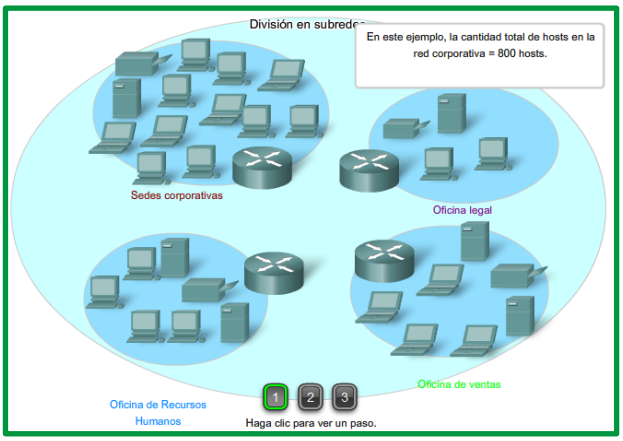


Figure 163. División de subredes. Paso 1 (determinar número de hosts)

Considere el ejemplo de una internetwork corporativa que necesita incluir 800 hosts en sus cuatro ubicaciones.

Determine la cantidad y el tamaño de las redes

A continuación, considere la cantidad de redes y el tamaño de cada una requeridas de acuerdo con los grupos comunes de hosts.

Paso 2.

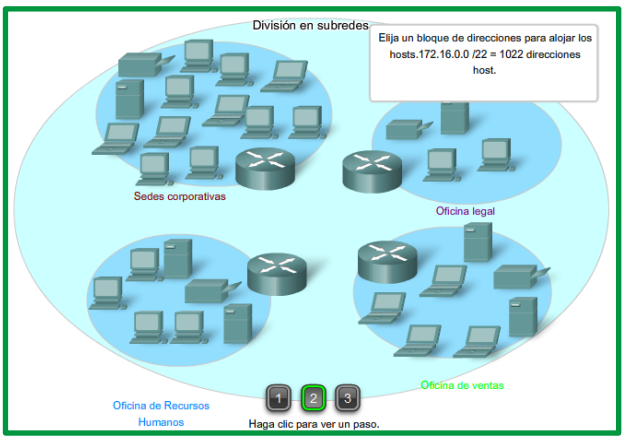


Figure 164. División de subredes. Paso 2 (determinar bloque de direcciones)

Se dividen las subredes de la red para superar problemas de ubicación, tamaño y control. Al diseñar el direccionamiento, se tienen en cuenta los factores para agrupar los hosts antes tratados:

- Agrupar basándonos en una ubicación geográfica común
- Agrupar hosts usados para propósitos específicos
- Agrupar basándonos en la propiedad

Cada enlace WAN es una red. Se crean subredes para la WAN que interconecta diferentes ubicaciones geográficas. Al conectar diferentes ubicaciones, se usa un router para dar cuenta de las diferencias de hardware entre las LAN y la WAN.

A pesar de que los hosts de una ubicación geográfica en común típicamente comprenden un solo bloque de direcciones, puede ser necesario realizar la división en subredes de este bloque para formar redes adicionales en cada ubicación. Es necesario crear subredes en diferentes ubicaciones que tengan hosts para las necesidades comunes de los usuarios. También puede suceder que otros grupos de usuarios requieran muchos recursos de red o que muchos usuarios requieran su propia subred. Además, es posible tener subredes para hosts especiales, como servidores. Es necesario tener en cuenta cada uno de estos factores para determinar la cantidad de redes.

También se deben tener en cuenta las necesidades de propiedad especiales de seguridad o administrativas que requieran redes adicionales.

Una herramienta útil para este proceso de planificación de direcciones es un diagrama de red. Un diagrama permite ver las redes y hacer una cuenta más precisa.

A fin de incluir 800 hosts en las cuatro ubicaciones de la compañía, se usa la aritmética binaria para asignar un bloque **/22** (2^10-2=1022).

Asignación de direcciones

Ahora que se conoce la cantidad de redes y la cantidad de hosts para cada red, es necesario comenzar a asignar direcciones a partir del bloque general de direcciones.

Paso 3.

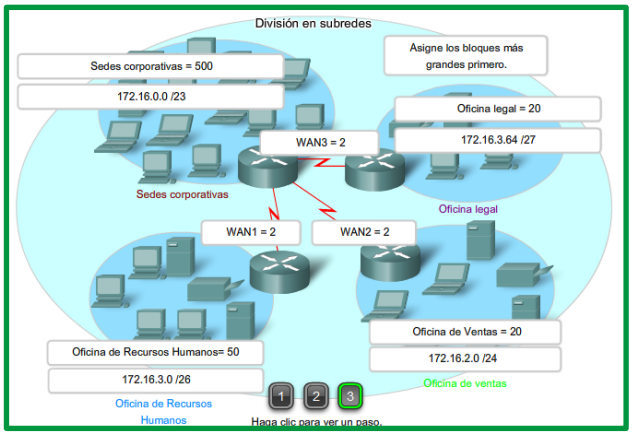


Figure 165. División de subredes. Paso 2 (determinación de cantidad de redes y host)

Este proceso comienza al asignar direcciones de red para ubicaciones de redes especiales. Se comienza por las ubicaciones que requieren la mayoría de los hosts y se continúa hasta los enlaces punto a punto. Este proceso asegura que se disponga de bloques de direcciones lo suficientemente amplios para incluir los hosts y las redes para estas ubicaciones.

Al hacer las divisiones y asignar las subredes disponibles, es necesario asegurarse de que haya direcciones del tamaño adecuado para mayores demandas. Además, se debe realizar una cuidadosa planificación para asegurar que los bloques de direcciones asignados a la subred no se superpongan.

Otra herramienta útil para este proceso de planificación es una hoja de cálculo. Es posible colocar las direcciones en columnas para visualizar la asignación de direcciones.

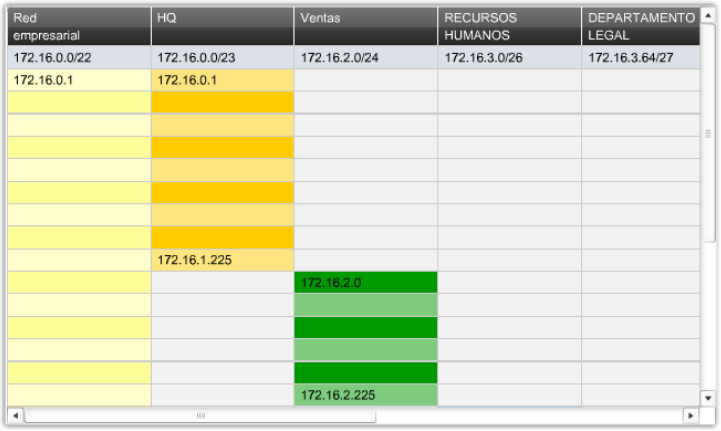


Figure 166. Proceso de planificación en una hoja de cálculo

En el ejemplo, se asignan bloques de direcciones a las cuatro ubicaciones, así como enlaces WAN.

Con los principales bloques asignados, se continúa realizando la división en subredes de cualquiera de las ubicaciones que requiera dicha división. En el ejemplo, se divide la sede corporativa en dos redes.

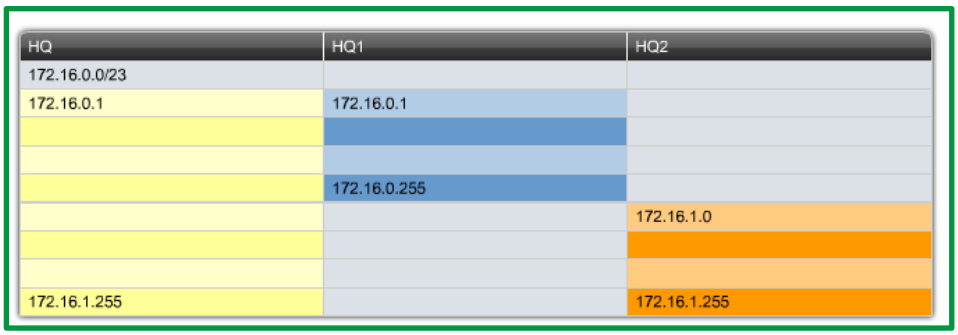


Figure 167. Proceso de planificación en una hoja de cálculo

Esta división adicional de las direcciones a menudo se llama división en subredes. Al igual que con la división en subredes, es necesario planificar detenidamente la asignación de direcciones de manera que se disponga de bloques de direcciones.

La creación de nuevas redes más pequeñas de un bloque de direcciones determinado se hace ampliando la longitud del prefijo; es decir, agregando números 1 a la máscara de subred. De esta forma se asignan más bits a la porción de red de la dirección para brindar más patrones para la nueva subred. Para cada bit que se pide prestado, se duplica la cantidad de redes. Por ejemplo: si se usa 1 bit, existe la posibilidad de dividir ese bloque en dos redes más pequeñas. Con un solo patrón de bit podemos producir dos patrones únicos de bit, 1 y 0. Si pedimos prestados 2 bits podemos proveer 4 patrones únicos para representar redes 00, 01, 10 y 11. Los 3 bits permitirían 8 bloques y así sucesivamente.

Número total de Hosts utilizables

Recuerde de la sección anterior que al dividir el rango de dirección en subredes perdimos dos direcciones de host para cada red nueva. Éstas son la dirección de red y la dirección de broadcast.

La fórmula para calcular el número de hosts en una red es:

Hosts utilizables = 2 n- 2

Donde n es el número de bits remanentes a ser utilizados por los hosts.

Enlaces:

Calculador de subred: http://vlsm-calc.net

Sumarización

La sumarización de rutas es una técnica empleada en enrutamiento IP avanzado que permite sintetizar múltiples rutas IP contiguas en una única ruta. De esta forma se obtienen varios beneficios:

- Se reduce la complejidad de las tablas de enrutamiento, reduciendo la cantidad de rutas.
- Se reduce el volumen de información de enrutamiento publicado.
- Se aumenta la estabilidad de las tablas de ruteo ya que una ruta sumaria permanece activa mientras al menos una de las rutas sumarizadas permanezca activa.
- Reduce los requerimientos de memoria RAM en los dispositivos ya que se reduce el tamaño de la tabla de ruteo.
- Reduce los requerimientos de procesamiento ya que minimiza los procedimientos de actualización de rutas y se reduce la cantidad de rutas a evaluar.

Un ejemplo de rutas sumarizadas:

Por ejemplo, se ha utilizado para identificar las VLANs de una sucursal de una empresa las subredes:

10.1.0.0/24

10.1.1.0/24

10.1.2.0/24

10.1.3.0/24

10.1.4.0/24

10.1.5.0/24

10.1.6.0/24

10.1.7.0/24

Por supuesto, en los dispositivos de la sucursal están presentes estas 8 rutas. Pero se desea que la sucursal publique la menor cantidad de rutas posibles hacia la casa central.

Para esto debemos sumarizar estas rutas. Estas 8 subredes pueden sumarizarse del modo más eficiente en una única ruta **/21** : 10.1.0.0/21

Se podría sumarizar en la 10.1.0.0/16, ciertamente es posible, el problema de esta última opción es que el rango de rutas sumarizado es mucho más amplio que las subredes existentes; si se tratara de subredes /24, esta ruta abarca cualquier subred /24 del rango 10.1.x.x.

Esta es una opción posible cuando se ha reservado ese rango de subredes para uso futuro en esa misma área. Pero no se puede utilizar cuando, por ejemplo, alguna de esas subredes está siendo utilizada en otra sucursal.

CIDR Y VLSM

La aplicación de un esquema de división en subredes tradicional a esta situación no resulta muy eficiente y genera desperdicio. La subdivisión de subredes, o el uso de una máscara de subred de longitud variable (VLSM), se diseñó para evitar que se desperdicien direcciones.

El sistema que utilizamos actualmente se denomina direccionamiento sin clase. Con el sistema classless, se asignan los bloques de direcciones adecuados para la cantidad de hosts a las compañías u organizaciones sin tener en cuenta la clase de unicast.

PLANIFICACIÓN DEL DIRECCIONAMIENTO DE RED

Es necesario que la asignación del espacio de direcciones de la capa de red dentro de la red corporativa esté bien diseñada. Los administradores de red no deben seleccionar de forma aleatoria las direcciones utilizadas en sus redes. Tampoco la asignación de direcciones dentro de la red debe ser aleatoria.

La asignación de estas direcciones dentro de las redes debería ser planificada y documentada a fin de:

- Evitar duplicación de direcciones.
- Proveer y controlar el acceso.
- Monitorear seguridad y rendimiento.

Evitar duplicación de direcciones

Como se sabe, cada host en una interwork debe tener una dirección única. Sin la planificación y documentación adecuadas de estas asignaciones de red, se podría fácilmente asignar una dirección a más de un host.

Brindar acceso y controlarlo

Algunos hosts ofrecen recursos tanto para la red interna como para la red externa. Un ejemplo de estos dispositivos son los servidores. El acceso a estos recursos puede ser controlado por la dirección de la Capa 3. Si las direcciones para estos recursos no son planificadas y documentadas, no es posible controlar fácilmente la seguridad y accesibilidad de los dispositivos. Por ejemplo: si se asigna una dirección aleatoria a un servidor, resulta difícil bloquear el acceso a su dirección y es posible que los clientes no puedan ubicar este recurso.

Monitorear la seguridad y el rendimiento

De igual manera, es necesario monitorear la seguridad y el rendimiento de los hosts de la red y de la red en general. Como parte del proceso de monitoreo, se examina el tráfico de la red mediante la búsqueda de direcciones que generan o reciben demasiados paquetes. Con una planificación y documentación correctas del direccionamiento de red, es posible identificar el dispositivo de la red que tiene una dirección problemática.

Asignación de direcciones dentro de una red

Como ya se ha mencionado, los hosts se asocian con una red IPv4 por medio de una porción de red en común de la dirección. Dentro de una red, existen diferentes tipos de hosts.

Algunos ejemplos de diferentes tipos de hosts son:

- Dispositivos finales para usuarios.
- Servidores y periféricos.
- Hosts a los que se accede desde Internet.
- Dispositivos intermediarios.

Cada uno de los diferentes tipos de dispositivos debe ser asignado en un bloque lógico de direcciones dentro del rango de direcciones de la red.

Una parte importante de la planificación de un esquema de direccionamiento IPv4 es decidir cuándo utilizar direcciones privadas y dónde se deben aplicar.

Se debe tener en cuenta lo siguiente:

> ¿Habrá más dispositivos conectados a la red que direcciones públicas asignadas por el ISP de la red?
>
> ¿Se necesitará acceder a los dispositivos desde fuera de la red local?
>
> Si los dispositivos a los que se pueden asignar direcciones privadas requieren acceso a Internet, ¿está la red capacitada para proveer el servicio de Traducción de dirección de red (NAT)?

Si hay más dispositivos que direcciones públicas disponibles, sólo esos dispositivos que accederán directamente a Internet, como los servidores Web, requieren una dirección pública. Un servicio NAT permitiría a esos dispositivos con direcciones privadas compartir de manera eficiente las direcciones públicas restantes.

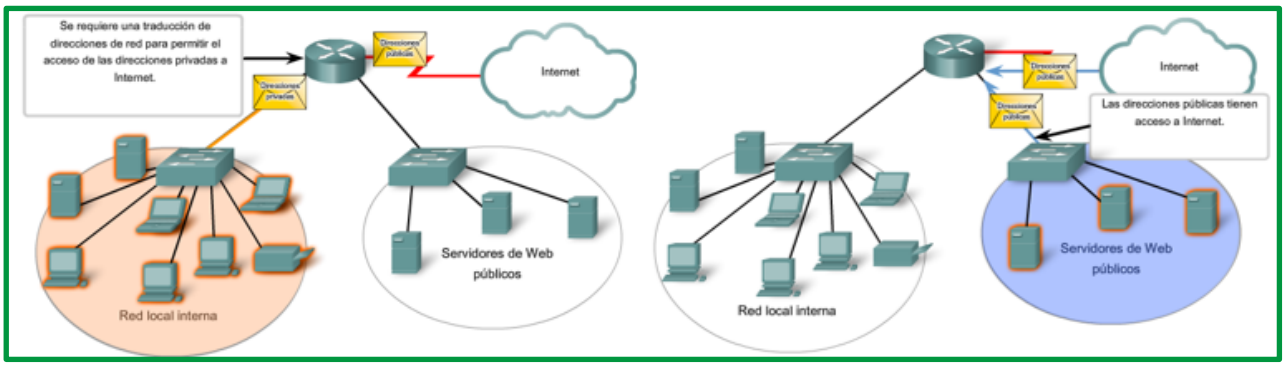


Figure 168. Planificación y asignación de direcciones IPv4 (Direcciones públicas y privadas)

CIDR.

El sistema que se utiliza en la actualidad se denomina “direccionamiento sin clase”. El nombre formal es “enrutamiento entre dominios sin clase” (CIDR, pronunciado “cider”). La asignación con clase de direcciones IPv4 era muy ineficaz, y permitía solo las duraciones de prefijo /8, /16 o /24, cada una de un espacio de dirección distinto. En 1993, el IETF creó un nuevo conjunto de estándares que permitía que los proveedores de servicios asignaran direcciones IPv4 en cualquier límite de bits de dirección (duración de prefijo) en lugar de solo con una dirección de clase A, B o C.

El IETF sabía que el CIDR era solo una solución temporal y que sería necesario desarrollar un nuevo protocolo IP para admitir el rápido crecimiento de la cantidad de usuarios de Internet. En 1994, el IETF comenzó a trabajar para encontrar un sucesor de IPv4, que finalmente fue IPv6.

Los ISP ya no están limitados a una máscara de subred de /8, /16 o /24. Ahora pueden asignar espacio de direcciones de manera más eficaz mediante el uso de cualquier longitud de prefijo que comience con /8 y valores superiores (es decir, /8, /9, /10, etc.). En la ilustración, se muestra de qué manera los bloques de direcciones IP se pueden asignar a una red en función de los requisitos del cliente, que pueden variar de unos pocos hosts a cientos o miles de hosts.

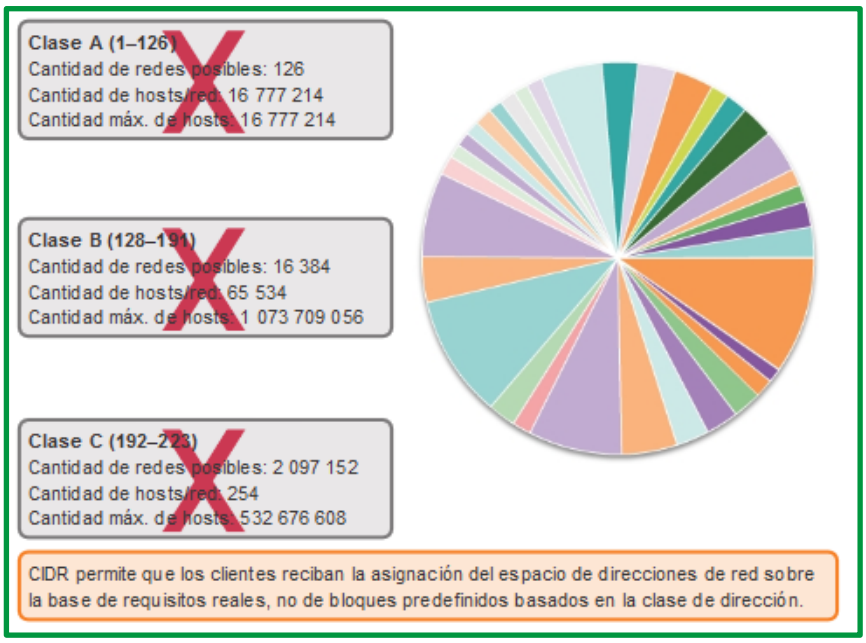


Figure 169. CIDR

El CIDR también reduce el tamaño de las tablas de routing y administra el espacio de direcciones IPv4 con mayor eficacia mediante:

- **Sumarización de ruta**: también conocida como “agregación de prefijos”. Las rutas se resumen en una única ruta para ayudar a reducir el tamaño de las tablas de routing. Por ejemplo, una ruta estática resumida puede reemplazar varias instrucciones de rutas estáticas específicas.
- **Creación de superredes**: ocurre cuando la máscara de sumarización de ruta es un valor menor que la máscara con clase predeterminada tradicional.

Una superred siempre es un resumen de rutas, pero un resumen de rutas no siempre es una superred.

En la ilustración, observe que el ISP1 tiene cuatro clientes y que cada uno tiene una cantidad variable de espacio de direcciones IP. El espacio de direcciones de los cuatro clientes puede resumirse en un anuncio para el ISP2. La ruta 192.168.0.0/20 resumida o agregada incluye todas las redes que pertenecen a los clientes A, B, C y D. Este tipo de ruta se conoce como “ruta de superred”. Una superred resume varias direcciones de red con una máscara menor que la máscara con clase.

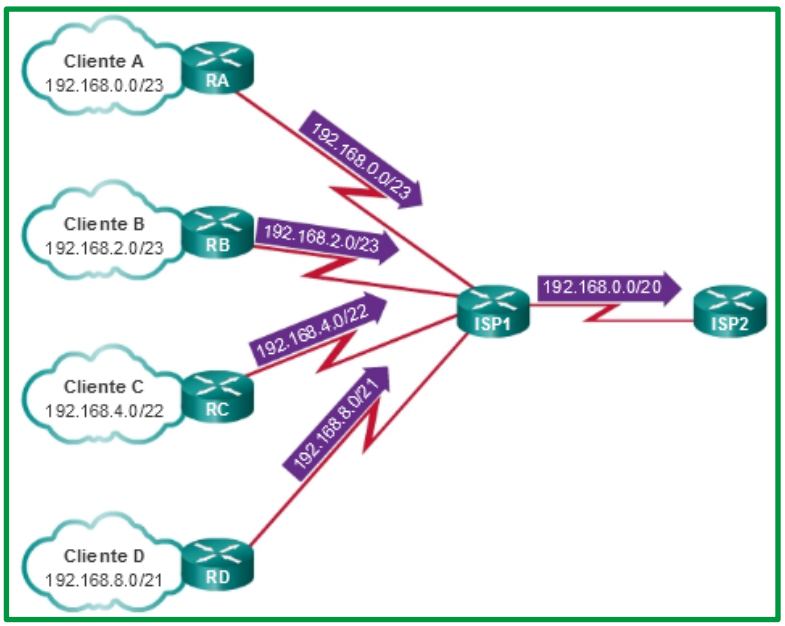


Figure 170. Resumen de rutas de supered

La determinación de la ruta resumida y la máscara de subred para un grupo de redes se puede realizar en tres pasos:

Paso 1. Enumere las redes en formato binario.

Paso 2. Cuente el número de bits coincidentes del extremo izquierdo. Esta es la longitud de prefijo o máscara de subred de la ruta resumida.

Paso 3. Copie los bits coincidentes y luego agregue los bits 0 al resto de la dirección para determinar la dirección de red resumida.

La dirección de red sumarizada y la máscara de subred ahora pueden usarse como ruta sumarizada para este grupo de redes. Las rutas resumidas pueden configurarse por medio de rutas estáticas y protocolos de routing sin clase.

La creación de tablas de enrutamiento más pequeñas hace que el proceso de búsqueda en la tabla de enrutamiento sea más eficaz ya que existen menos rutas para buscar. Si se puede utilizar una ruta estática en lugar de varias, se reduce el tamaño de la tabla de routing. En muchos casos, se puede usar una sola ruta estática para representar docenas, cientos o incluso miles de rutas.

Las rutas resumidas CIDR se pueden configurar mediante rutas estáticas. Esto contribuye a reducir el tamaño de las tablas de routing.

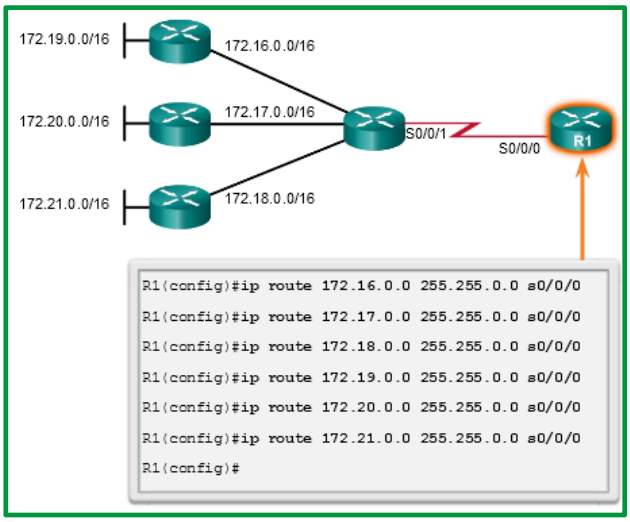


Figure 171. Seis rutas estáticas configuradas en R1

En la figura anterior, el R1 se configuró para alcanzar las redes identificadas en la topología. Si bien es aceptable, sería más eficaz configurar una ruta estática resumida.

En la figura siguiente, se proporciona una solución con utilizando la sumarización CIDR. Las seis entradas de ruta estática se podrían reducir a la entrada 172.16.0.0/13. En el ejemplo, se eliminan las seis entradas de ruta estática y se las reemplaza con una ruta estática resumida

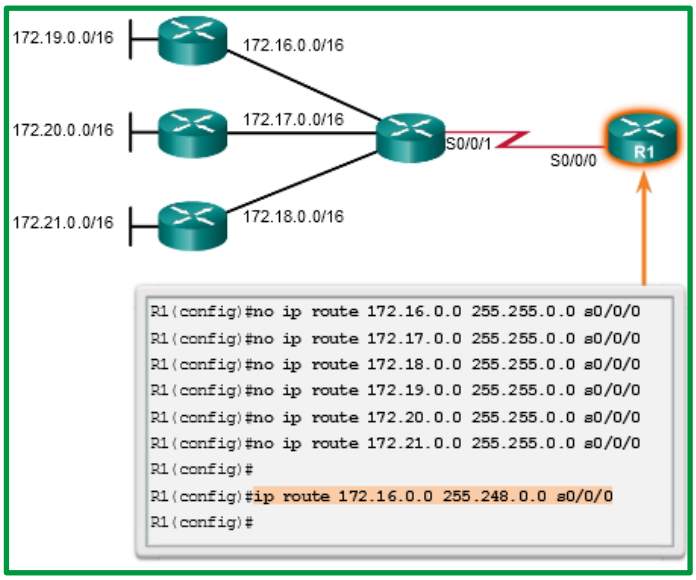


Figure 172. Aplicación de ruta estática resumida

Los protocolos de routing con clase no pueden enviar rutas de superred. Esto se debe a que el router receptor aplica de forma automática la máscara de subred con clase predeterminada a la dirección de red en la actualización de routing. Si la topología en la ilustración tuviera un

protocolo de routing con clase, entonces el R3 solo instalaría 172.16.0.0/16 en la tabla de routing.

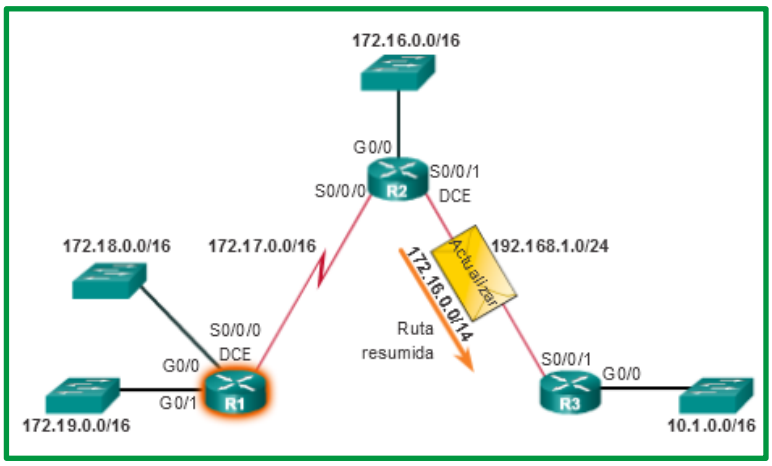


Figure 173. Topología de referencia para explicación de rutas VLSM

La propagación de las rutas VLSM y de superred requiere un protocolo de routing sin clase, como RIPv2, OSPF o EIGRP. Los protocolos de routing sin clase anuncian las direcciones de red junto con las máscaras de subred asociadas. Con un protocolo de routing sin clase, el R2 puede resumir las redes 172.16.0.0/16, 172.17.0.0/16, 172.18.0.0/16 y 172.19.0.0/16, y anunciar una ruta estática resumida de superred 172.16.0.0/14 al R3. A continuación, el R3 instala la ruta de superred 172.16.0.0/14 en la tabla de routing.

Sabías que. - Cuando una ruta de superred se encuentra en una tabla de routing, por ejemplo, como una ruta estática, un protocolo de routing con clase no incluye esa ruta en las actualizaciones.

VLSM

Con la máscara de subred de longitud fija (FLSM), se asigna la misma cantidad de direcciones a cada subred. Si todas las subredes tuvieran los mismos requisitos en cuanto a la cantidad de hosts, estos bloques de direcciones de tamaño fijo serían suficientes. Sin embargo, esto no es lo que suele suceder.

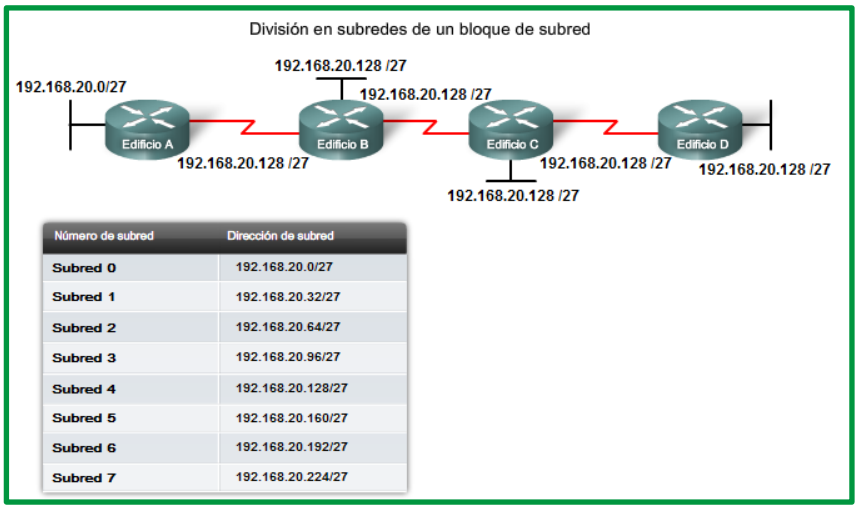
Clases de direcciones IP

Clase de direcciones	1er rango del octeto (decimal)	1eros bits del octeto (los bits verdes no cambian)	Partes de las direcciones de red(N) y de host(H)	Máscara de subred predeterminada (decimal y binaria)	Número de posibles redes y hosts por red
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 redes (2^7) 16,777,214 hosts por red (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 redes (2^14) 65,534 hosts por red (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,150 redes (2^21) 254 hosts por red (2^8-2)
D	224-239	11000000-11011111	ND (multicast)		
E	240-255	11110000-11111111	ND (experimental)		

** Todos los ceros (0) y los unos (1) son direcciones hosts no válidas.

Figure 174. División de direcciones IP con clases

La subdivisión en subredes, o el uso de una Máscara de subred de longitud variable (VLSM), fue diseñada para maximizar la eficiencia del direccionamiento. Al identificar la cantidad total de hosts que utiliza la división tradicional en subredes, se asigna la misma cantidad de direcciones para cada subred. Si todas las subredes tuvieran los mismos requisitos en cuanto a la cantidad de hosts, estos bloques de direcciones de tamaño fijo serían eficientes. Sin embargo, esto no es lo que suele suceder.



Número de subred	Dirección de subred
Subred 0	192.168.20.0/27
Subred 1	192.168.20.32/27
Subred 2	192.168.20.64/27
Subred 3	192.168.20.96/27
Subred 4	192.168.20.128/27
Subred 5	192.168.20.160/27
Subred 6	192.168.20.192/27
Subred 7	192.168.20.224/27

Figure 175. Topología con 8 subredes

Por ejemplo: la topología en la figura muestra los requisitos de subred de siete subredes, una para cada una de las cuatro LAN y una para cada una de las tres WAN. Con la dirección 192.168.20.0, es necesario pedir prestados 3 bits de los bits del host en el último octeto para satisfacer los requisitos de subred de siete subredes.

Estos bits son bits que se toman prestados al cambiar la máscara de subred correspondiente por números "1" para indicar que estos bits ahora se usan como bits de red. Entonces, el último

octeto de la máscara se representa en binario con 11100000, que es 224. La nueva máscara 255.255.255.224 se representa mediante la notación /27 para representar un total de 27 bits para la máscara.

En binario, esta máscara de subred se representa como: 11111111.11111111.11111111.11100000

Luego de tomar prestados tres de los bits de host para usar como bits de red, quedan cinco bits de host. Estos cinco bits permitirán más de 30 hosts por subred.

A pesar de que se ha cumplido la tarea de dividir la red en una cantidad adecuada de redes, esto se hizo mediante la pérdida significativa de direcciones no utilizadas. Por ejemplo: sólo se necesitan dos direcciones en cada subred para los enlaces WAN. Hay 28 direcciones no utilizadas en cada una de las tres subredes WAN que han sido bloqueadas en estos bloques de direcciones. Además, de esta forma se limita el crecimiento futuro al reducir el número total de subredes disponibles. Este uso ineficiente de direcciones es característico del direccionamiento con clase.

La aplicación de un esquema de división en subredes tradicional a esta situación no resulta muy eficiente y genera desperdicio. De hecho, este ejemplo es un modelo satisfactorio para mostrar cómo la división en subredes de una subred puede utilizarse para maximizar el uso de la dirección. La subdivisión de subredes, o el uso de una máscara de subred de longitud variable (VLSM), se diseñó para evitar que se desperdicien direcciones.

En la división en subredes tradicional se aplica la misma máscara de subred a todas las subredes. Esto significa que cada subred tiene la misma cantidad de direcciones de host disponibles.

Con VLSM, la longitud de la máscara de subred varía según la cantidad de bits que se toman prestados para una subred específica, de lo cual deriva la parte “variable” de la máscara de subred de longitud variable. Como se muestra en la figura siguiente, VLSM permite dividir un espacio de red en partes desiguales.

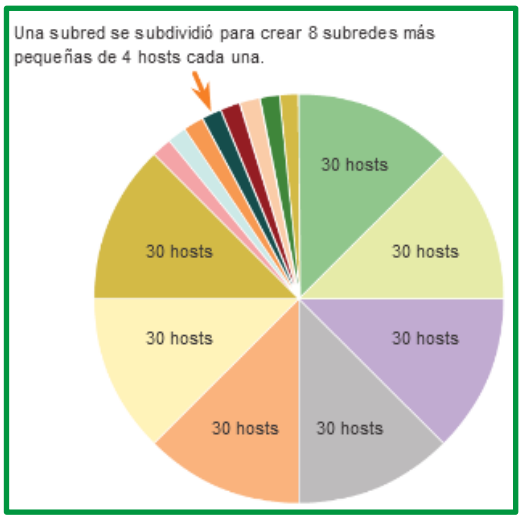


Figure 176. Subredes de distinto tamaño

La división en subredes de VLSM es similar a la división en subredes tradicional en cuanto a que se toman prestados bits para crear subredes. Las fórmulas para calcular la cantidad de hosts por

subred y la cantidad de subredes que se crean también son válidas para VLSM. La diferencia es que la división en subredes no es una actividad que conste de un único paso. Con VLSM, la red primero se divide en subredes y, a continuación, las subredes se vuelven a dividir en subredes. Este proceso se puede repetir varias veces crear subredes de diversos tamaños.

VLSM permite el uso de diferentes máscaras para cada subred. Después de que una dirección de red se divide en subredes, esas subredes también se pueden dividir en subredes. VLSM simplemente subdivide una subred. Se puede considerar a VLSM como una división en sub-subredes.

Obtención de más subredes para menos hosts

Como se mostró en ejemplos anteriores, se comenzó con las subredes originales y se obtuvieron subredes adicionales más pequeñas para usar en los enlaces WAN. Creando subredes más pequeñas, cada subred puede soportar 2 hosts, dejando libres las subredes originales para ser asignadas a otros dispositivos y evitando que muchas direcciones puedan ser desperdiciadas.

Para crear estas subredes más pequeñas para los enlaces WAN, comience con 192.168.20.192. Podemos dividir esta subred en subredes más pequeñas. Para suministrar bloques de direcciones para las WAN con dos direcciones cada una, se tomarán prestados tres bits de host adicionales para usar como bits de red.

Dirección: 192.168.20.192 En binario: 11000000.10101000.00010100.11000000

Máscara: 255.255.255.252 30 bits en binario: 11111111.11111111.11111111.11111100

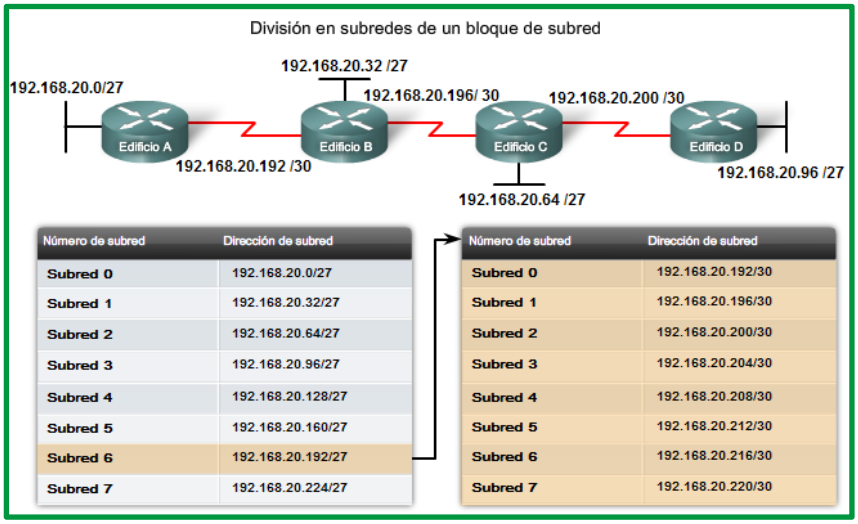


Figure 177. VLSM como una división en sub-subredes

La topología en la figura muestra un plan de direccionamiento que divide las subredes 192.168.20.192 /27 en subredes más pequeñas para suministrar direcciones para las WAN. De esta forma se reduce la cantidad de direcciones por subred a un tamaño apropiado para las WAN. Con este direccionamiento, se obtienen subredes 4, 5 y 7 disponibles para futuras redes, así como varias subredes disponibles para las WAN.

Ejemplo practico

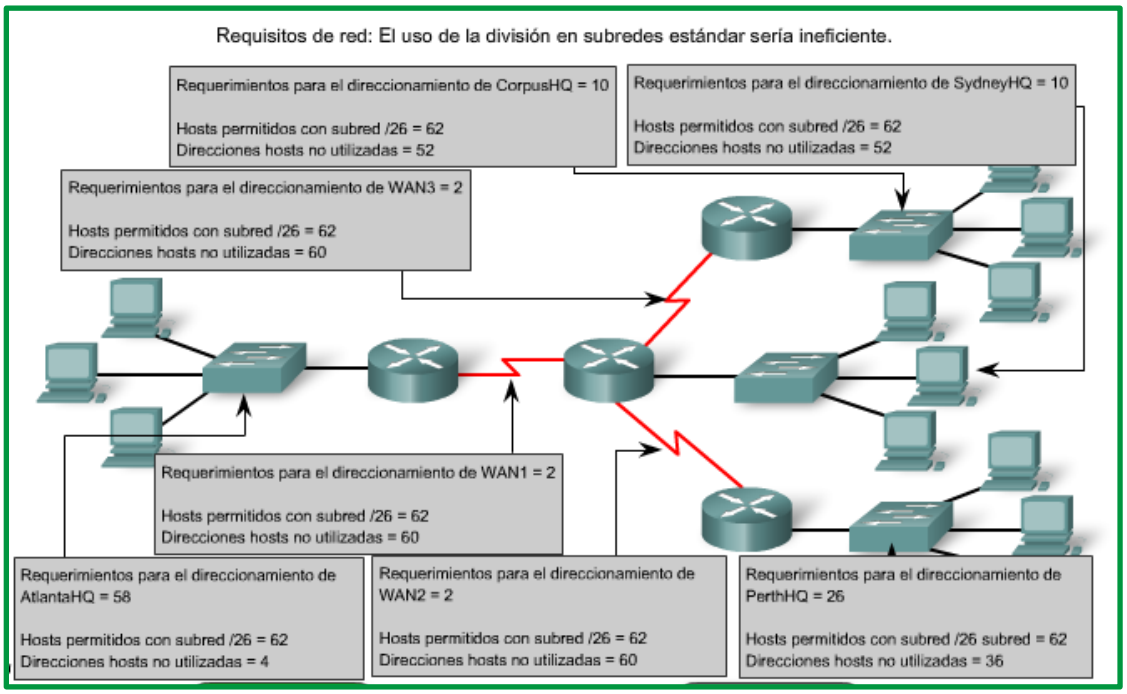


Figure 178. Topología de ejemplo práctico

En la figura anterior se considerará el direccionamiento desde otra perspectiva. Se tendrá en cuenta la división en subredes de acuerdo con la cantidad de hosts, incluso las interfaces de router y las conexiones WAN. Este escenario posee los siguientes requisitos:

- AtlantaHQ 58 direcciones de host
- PerthHQ 26 direcciones de host
- SydneyHQ 10 direcciones de host
- CorpusHQ 10 direccciones de host
- Enlaces WAN 2 direcciones de host (cada una)

	Requisitos actuales	Desperdicio total de direcciones
AtlantaHQ	58 direcciones de host	4 direcciones
PerthHQ	26 direcciones de host	36 direcciones
SydneyHQ	10 direcciones de host	52 direcciones
CorpusHQ	10 direcciones de host	52 direcciones
Enlaces WAN	2 direcciones de host (cada una)	60 direcciones

Figure 179. Requisitos de host

Queda claro que, a partir de estos requerimientos, el uso de un esquema de armado estándar de subredes sería un gran desperdicio. En esta internetwork, el armado estándar de subredes bloquearía cada subred en bloques de 62 hosts, lo que llevaría a un significativo desperdicio de direcciones potenciales. Este desperdicio es especialmente evidente en la figura anterior, donde se ve que la LAN PerthHQ admite 26 usuarios y que los routers de LAN SydneyHQ y CorpusHQ admiten 10 usuarios cada uno.

Por lo tanto, con el bloque de direcciones 192.168.15.0 /24 se comenzará a diseñar un esquema de direccionamiento que cumpla los requisitos y guarde posibles direcciones.

Obtención de más direcciones

Al crear un esquema de direccionamiento adecuado, siempre se comienza con la mayor demanda. En este caso, AtlantaHQ, con 58 usuarios, tiene la mayor demanda. A partir de 192.168.15.0, se precisarán 6 bits de host para incluir la demanda de 58 hosts; esto deja 2 bits adicionales para la porción de red. El prefijo para esta red sería /26 y la máscara de subred 255.255.255.192.

Comencemos por dividir en subredes el bloque original de direcciones 192.168.15.0 /24. Al usar la fórmula de hosts utilizables = 2^n - 2, se calcula que 6 bits de host permiten 62 hosts en la subred. Los 62 hosts satisfarían los 58 hosts requeridos del router de la compañía AtlantaHQ.

Dirección: 192.168.15.0

En binario: 11000000.10101000.00001111.00000000

Máscara: 255.255.255.192

26 bits en binario: 11111111.11111111.11111111.11000000

Aquí se describen los pasos para implementar este esquema de armado de subredes.

Asignar la LAN de AtlantaHQ

Nombre - dirección requerida	Dirección de subred	Rango de dirección	Dirección de broadcast	Red/prefijo
AtlantaHQ - 58	192.168.15.0	.1 - .62	.63	192.168.15.0 /26
PerthHQ - 28				
SydneyHQ - 10				
CorpusHQ - 10				
WAN1 - 2				
WAN2 - 2				
WAN3 - 2				

Calcule la máscara de subred para cumplir con el requisito más grande - AtlantaHQ

Figure 180. Datos de entrada para AtlantaHQ

El primer paso mostró un gráfico de planificación de red. El segundo paso en la figura muestra la entrada para AtlantaHQ. Esta entrada es el resultado del cálculo de una subred a partir del bloque original 192.168.15.0 /24 a fin de incluir la LAN más grande, la LAN AtlantaHQ con 58 hosts. Para realizar esta acción fue necesario pedir prestados 2 bits de host adicionales, para usar una máscara de bits /26.

Al compararlo, el siguiente esquema muestra cómo 192.168.15.0 se dividiría en subredes mediante el bloque de direccionamiento fijo para brindar bloques de direcciones lo suficientemente amplios:

- Subred 0: 192.168.15.0 /26 rango de direcciones host de 1 a 62
- Subred 1: 192.168.15.64 /26 rango de direcciones host de 65 a 126
- Subred 2: 192.168.15.128 /26 rango de direcciones host de 129 a 190
- Subred 3: 192.168.15.192 /26 rango de direcciones host de 193 a 254

Los bloques fijos permitirían sólo cuatro subredes y, por lo tanto, no dejarían suficientes bloques de direcciones para la mayoría de las subredes de esta internetwork. En lugar de continuar utilizando la siguiente subred disponible, es necesario asegurarse de que el tamaño de cada subred sea consecuente con los requisitos de host. Para usar un esquema de direccionamiento que se relacione directamente con los requisitos de host se debe usar un método diferente de división en subredes.

Asignación de la LAN PerthHQ

Nombre - dirección requerida	Dirección de subred	Rango de dirección	Dirección de broadcast	Red/prefijo
AtlantaHQ - 58	192.168.15.0	.1 - .62	.63	192.168.15.0 /26
PerthHQ - 28	192.168.15.64	.65 - .94	.95	192.168.15.64 /27
SydneyHQ - 10				
CorpusHQ - 10				
WAN1 - 2				
WAN2 - 2				
WAN3 - 2				

Utilice la próxima dirección disponible .64 para calcular una máscara de subred para el próximo requisito más grande - PerthHQ.

Figure 181. Asignación de la LAN PerthHQ

En el tercer paso, se observan los requisitos de la siguiente subred más grande. Ésta es la LAN PerthHQ, que requiere 28 direcciones de host, incluida la interfaz de router. Se debe comenzar con la siguiente dirección disponible 192.168.15.64 para crear un bloque de direcciones para esta subred. Al pedir prestado otro bit, se pueden satisfacer las necesidades de PerthHQ al tiempo que se limita el desperdicio de direcciones. El bit tomado deja una máscara /27 con el siguiente intervalo de direcciones:

192.168.15.64 /27 intervalo de direcciones de host 65 a 94

Este bloque de direcciones suministra 30 direcciones, lo cual satisface la necesidad de 28 hosts y deja espacio para el crecimiento de esta subred.

Asignación de las LAN SydneyHQ y CorpusHQ

Nombre - dirección requerida	Dirección de subred	Rango de dirección	Dirección de broadcast	Red/prefijo
AtlantaHQ - 58	192.168.15.0	.1 - .62	.63	192.168.15.0 /26
PerthHQ - 28	192.168.15.64	.65 - .94	.95	192.168.15.64 /27
SydneyHQ - 10	192.168.15.96	.97 - .110	.111	192.168.15.96 /28
CorpusHQ - 10	192.168.15.112	.113 - .126	.127	192.168.15.112 /28
WAN1 - 2				
WAN2 - 2				
WAN3 - 2				

Utilice la próxima dirección disponible .112 para calcular una subred para CorpusHQ que también requiere 10 hosts.

Figure 182. Asignación de las LAN SydneyHQ y CorpusHQ

Los pasos cuatro y cinco proporcionan direccionamiento para las siguientes subredes más grandes: Las LAN SydneyHQ y CorpusHQ. En estos dos pasos, cada LAN tiene la misma necesidad de 10 direcciones host. Esta división en subredes requiere tomar prestado otro bit, a fin de ampliar la máscara a /28. A partir de la dirección 192.168.15.96, se obtienen los siguientes bloques de direcciones:

- Subred 0: 192.168.15.96 /28 rango de direcciones host de 97 a 110
- Subred 1: 192.168.15.112 /28 rango de direcciones host de 113 a 126

Estos bloques proporcionan 14 direcciones para los hosts y las interfaces del router para cada LAN.

Asignación de las WAN

Nombre - dirección requerida	Dirección de subred	Rango de dirección	Dirección de broadcast	Red/prefijo
AtlantaHQ - 58	192.168.15.0	.1 - .62	.63	192.168.15.0 /26
PerthHQ - 28	192.168.15.64	.65 - .94	.95	192.168.15.64 /27
SydneyHQ - 10	192.168.15.96	.97 - .110	.111	192.168.15.96 /28
CorpusHQ - 10	192.168.15.112	.113 - .126	.127	192.168.15.112 /28
WAN1 - 2	192.168.15.128	.129 - .130	.131	192.168.15.128 /30
WAN2 - 2	192.168.15.132	.133 - 134	.135	192.168.15.132 /30
WAN3 - 2	192.168.15.136	.137 - .138	.139	192.168.15.136 /30

El problema de red está solucionado

Figure 183. Asignación de las WAN

Los últimos pasos muestran la división en subredes para los enlaces WAN. Con estos enlaces WAN punto a punto, sólo se necesitan dos direcciones. Con el objetivo de satisfacer los

requisitos, se toman 2 bits más para usar una máscara /30. Al utilizar las próximas direcciones disponibles, se obtienen los siguientes bloques de direcciones:

- Subred 0: 192.168.15.128 /30 rango de direcciones host de 129 a 130
- Subred 1: 192.168.15.132 /30 rango de direcciones host de 133 a 134
- Subred 2: 192.168.15.136 /30 rango de direcciones host de 137 a 138

Los resultados muestran en nuestro esquema de direccionamiento, usando visualizaciones VLSM, una amplia gama de bloques de direcciones correctamente asignados. Como una mejor práctica, se comenzó por documentar los requisitos, de mayor a menor. Al comenzar por el requisito mayor, fue posible determinar que un esquema de bloque de direccionamiento fijo no permitiría un uso eficiente de las direcciones IPv4 y, como se muestra en este ejemplo, no suministraría suficientes direcciones.

Se tomaron prestados bits del bloque de direcciones asignado para crear los intervalos de direcciones que se ajusten a la topología. La figura anterior se muestra los intervalos asignados. La figura siguiente muestra la topología con la información de direccionamiento.

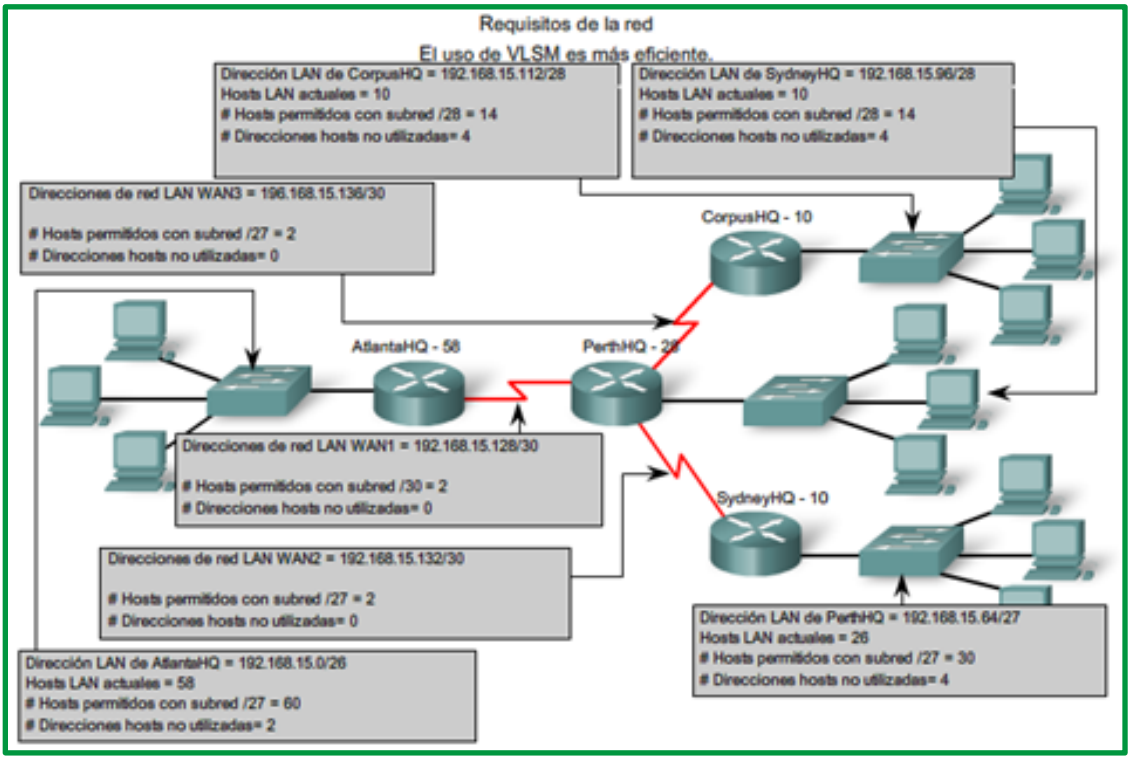


Figure 184. Topología de red aplicando VLSM

El uso de **VLSM** para asignar las direcciones permitió aplicar las guías de división en subredes para agrupar hosts según:

- Agrupación basada en ubicación geográfica común
- Agrupación de hosts utilizados para propósitos específicos
- Agrupación basada en propiedad

Cuadro de VLSM

También se puede realizar la planificación de direcciones utilizando diversas herramientas. Un método es utilizar un cuadro de VLSM para identificar los bloques de direcciones disponibles para su uso y los que ya están asignados. Este método ayuda a evitar la asignación de direcciones que ya han sido asignadas. Con la red del ejemplo, es posible inspeccionar la planificación de direcciones usando el cuadro de VLSM para ver su uso.

El primer gráfico muestra la porción superior del cuadro. Un cuadro completo para su uso está disponible utilizando el enlace a continuación.

https://drive.google.com/file/d/1D7FCi1gTdYN-tXaygUqJABcYl9guUxfC/view?usp=sharing

Este cuadro se puede usar para planificar direcciones para redes con prefijos en el rango de /25 - /30. Éstos son los rangos de red de uso más frecuente para la división en subredes.

El proceso realizado anteriormente también se puede realizar aplicando el cuadro VLSM, se captura a modo de ejemplos las pantallas de proceso en cada asignación.

<table>
<tr><th></th><th>/25 (subred de 1 bit)
subred de 2 bits
126 hosts</th><th>/26 (subred de 2 bits)
4 máscaras de subred</th><th>/27 (subred de 3 bits)
8 subredes
30 hosts</th><th>/28 (subred de 4 bits)
16 subredes
14 hosts</th><th>/29 (subred de 5 bits)
32 subredes
6 hosts</th><th>/30 (subred de 6 bits)
64 subredes
2 hosts</th></tr>
<tr><td>.0</td><td rowspan="32">.0</td><td rowspan="16">Bloquear
AtlantaHQ

.0 (.1-.62)</td><td rowspan="8">.0 (.1-.30)</td><td rowspan="4">.0 (.1-.14)</td><td>.0 (.1-.6)</td><td>.0 (.1-.2)
.4 (.5-.6)</td></tr>
<tr><td>.4</td></tr>
<tr><td>.8</td><td>.8 (.9 - .14)</td><td>.8 (.9 - .10)
.12 (.13-.14)</td></tr>
<tr><td>.12</td></tr>
<tr><td>.16</td><td rowspan="4">.16 (.17-.30)</td><td>.16 (.17-.22)</td><td>.16 (.17-.18)
.20 (.21-.22)</td></tr>
<tr><td>.20</td></tr>
<tr><td>.24</td><td>.24 (.25-.30)</td><td>.24 (.25-.26)
.28 (.29-.30)</td></tr>
<tr><td>.28</td></tr>
<tr><td>.32</td><td rowspan="8">.32 (.33-.62)</td><td rowspan="4">.32 (.33-.46)</td><td>.32 (.33-.38)</td><td>.32 (.33-.34)
.36 (.37-.38)</td></tr>
<tr><td>.36</td></tr>
<tr><td>.40</td><td>.40 (.41-.46)</td><td>.40 (.41-.42)
.44 (.45-.46)</td></tr>
<tr><td>.44</td></tr>
<tr><td>.48</td><td rowspan="4">.48 (.49-.62)</td><td>.48 (.49-.54)</td><td>.48 (.49-.50)
.52 (.53-.54)</td></tr>
<tr><td>.52</td></tr>
<tr><td>.56</td><td>.56 (.57-.62)</td><td>.56 (.57-.58)
.60 (.61-.62)</td></tr>
<tr><td>.60</td></tr>
<tr><td>.64</td><td rowspan="16">.64 (.65-.126)</td><td rowspan="8">.64 (.65-.94)</td><td rowspan="4">.64 (.65-.78)</td><td>.64 (.65-.70)</td><td>.64 (.65-.66)
.68 (.69-.70)</td></tr>
<tr><td>.68</td></tr>
<tr><td>.72</td><td>.72 (.73-.78)</td><td>.72 (.73-.74)
.76 (.77-.78)</td></tr>
<tr><td>.76</td></tr>
<tr><td>.80</td><td rowspan="4">.80 (.81-.94)</td><td>.80 (.81-.86)</td><td>.80 (.81-.82)
.84 (.85-.86)</td></tr>
<tr><td>.84</td></tr>
<tr><td>.88</td><td>.88 (.89-.94)</td><td>.88 (.89-.90)
.92 (.93-.94)</td></tr>
<tr><td>.92</td></tr>
<tr><td>.96</td><td rowspan="8">.96 (.97-.126)</td><td rowspan="4">.96 (.97-.110)</td><td>.96 (.97-.102)</td><td>.96 (.97-.98)
.100 (.101-.102)</td></tr>
<tr><td>.100</td></tr>
<tr><td>.104</td><td>.104 (.105-.110)</td><td>.104 (.105-.106)
.108 (.109-.110)</td></tr>
<tr><td>.108</td></tr>
<tr><td>.112</td><td rowspan="4">.112 (.113-.126)</td><td>.112 (.113-.118)</td><td>.112 (.113-.114)
.116 (.117-.118)</td></tr>
<tr><td>.116</td></tr>
<tr><td>.120</td><td>.120 (.121-.126)</td><td>.120 (.121-.122)
.124 (.125-.126)</td></tr>
<tr><td>.124</td></tr>
</table>

Figure 185. Elección de un bloque de la LAN AtlantaHQ aplicando el cuadro VLSM

/25 (subred de 1 bit) subred de 2 bits 126 hosts		/26 (subred de 2 bits) 4 máscaras de subred	/27 (subred de 3 bits) 8 subredes 30 hosts	/28 (subred de 4 bits) 16 subredes 14 hosts	/29 (subred de 5 bits) 32 subredes 6 hosts	/30 (subred de 6 bits) 64 subredes 2 hosts
.0	Dirección asignada	.0 (.1-.62)	.0 (.1-.30)	.0 (.1-.14)	.0 (.1-.6)	.0 (.1-.2)
.4						.4 (.5-.6)
.8					.8 (.9 - .14)	.8 (.9 - .10)
.12						.12 (.13-.14)
.16				.16 (.17-.30)	.16 (.17-.22)	.16 (.17-.18)
.20						.20 (.21-.22)
.24					.24 (.25-.30)	.24 (.25-.26)
.28						.28 (.29-.30)
.32			.32 (.33-.62)	.32 (.33-.46)	.32 (.33-.38)	.32 (.33-.34)
.36						.36 (.37-.38)
.40					.40 (.41-.46)	.40 (.41-.42)
.44						.44 (.45-.46)
.48				.48 (.49-.62)	.48 (.49-.54)	.48 (.49-.50)
.52						.52 (.53-.54)
.56					.56 (.57-.62)	.56 (.57-.58)
.60						.60 (.61-.62)
.64	.0	.64 (.65-.126)	Bloquear PerthHQ .64 (.65-.94)	.64 (.65-.78)	.64 (.65-.70)	.64 (.65-.66)
.68						.68 (.69-.70)
.72					.72 (.73-.78)	.72 (.73-.74)
.76						.76 (.77-.78)
.80				.80 (.81-.94)	.80 (.81-.86)	.80 (.81-.82)
.84						.84 (.85-.86)
.88					.88 (.89-.94)	.88 (.89-.90)
.92						.92 (.93-.94)
.96			.96 (.97-.126)	.96 (.97-.110)	.96 (.97-.102)	.96 (.97-.98)
.100						.100 (.101-.102)
.104					.104 (.105-.110)	.104 (.105-.106)
.108						.108 (.109-.110)
.112				.112 (.113-.126)	.112 (.113-.118)	.112 (.113-.114)
.116						.116 (.117-.118)
.120					.120 (.121-.126)	.120 (.121-.122)
.124						.124 (.125-.126)

Figure 186. Elección de un bloque para la LAN PerthHQ aplicando cuadro VLSM

/25 (subred de 1 bit) subred de 2 bits 126 hosts		/26 (subred de 2 bits) 4 máscaras de subred	/27 (subred de 3 bits) 8 subredes 30 hosts	/28 (subred de 4 bits) 16 subredes 14 hosts	/29 (subred de 5 bits) 32 subredes 6 hosts	/30 (subred de 6 bits) 64 subredes 2 hosts
.0	Dirección asignada	.0 (.1-.62)	.0 (.1-.30)	.0 (.1-.14)	.0 (.1-.6)	.0 (.1-.2)
.4						.4 (.5-.6)
.8					.8 (.9 - .14)	.8 (.9 - .10)
.12						.12 (.13-.14)
.16				.16 (.17-.30)	.16 (.17-.22)	.16 (.17-.18)
.20						.20 (.21-.22)
.24					.24 (.25-.30)	.24 (.25-.26)
.28						.28 (.29-.30)
.32			.32 (.33-.62)	.32 (.33-.46)	.32 (.33-.38)	.32 (.33-.34)
.36						.36 (.37-.38)
.40					.40 (.41-.46)	.40 (.41-.42)
.44						.44 (.45-.46)
.48				.48 (.49-.62)	.48 (.49-.54)	.48 (.49-.50)
.52						.52 (.53-.54)
.56					.56 (.57-.62)	.56 (.57-.58)
.60						.60 (.61-.62)
.64	.0	.64 (.65-.126)	.64 (.65-.94)	.64 (.65-.78)	.64 (.65-.70)	.64 (.65-.66)
.68						.68 (.69-.70)
.72					.72 (.73-.78)	.72 (.73-.74)
.76						.76 (.77-.78)
.80				.80 (.81-.94)	.80 (.81-.86)	.80 (.81-.82)
.84						.84 (.85-.86)
.88					.88 (.89-.94)	.88 (.89-.90)
.92						.92 (.93-.94)
.96			Bloquear SydneyHQ .96 (.97-.126) Bloquear CorpusHQ	.96 (.97-.110)	.96 (.97-.102)	.96 (.97-.98)
.100						.100 (.101-.102)
.104					.104 (.105-.110)	.104 (.105-.106)
.108						.108 (.109-.110)
.112				.112 (.113-.126)	.112 (.113-.118)	.112 (.113-.114)
.116						.116 (.117-.118)
.120					.120 (.121-.126)	.120 (.121-.122)
.124						.124 (.125-.126)

Figure 187. Elección de bloques para la LAN de SydneyHQ y la LAN de CorpusHQ aplicando cuadro VLSM

/25 (subred de 1 bit) subred de 2 bits 126 hosts		/26 (subred de 2 bits) 4 máscaras de subred	/27 (subred de 3 bits) 8 subredes 30 hosts	/28 (subred de 4 bits) 16 subredes 14 hosts	/29 (subred de 5 bits) 32 subredes 6 hosts	/30 (subred de 6 bits) 64 subredes 2 hosts
.128	.128	.128 (.129-.190)	.128 (.129-.158)	.128 (.129-.142)	WAN bloquea (3)	.128 (.129-.130)
.132						.132 (.133-.134)
.136					.136 (.137-.142)	.136 (.137-.138)
.140						.140 (.141-.142)
.144				.144 (.145-.158)	.144 (.145-.150)	.144 (.145-.146)
.148						.148 (.149-.150)
.152					.152 (.153-.158)	.152 (.153-.154)
.156						.156 (.157-.158)
.160			.160 (.161-.190)	.160 (.161- 174)	.160 (.161-.166)	.160 (.161-.162)
.164						.164 (.165-.166)
.168					.168 (.169-.174)	.168 (.169-.170)
.172						.172 (.173-.174)
.176				.176 (.177-.190)	.176 (.177-.182)	.176 (.177-.178)
.180						.180 (.181-.182)
.184					.184 (.185-.190)	.184 (.185-.186)
.188						.188 (.189-.190)
.192		.192 (.193-.254)	.192 (.193-.222)	.192 (.193-.206)	.192 (.193-.202)	.192 (.193-.194)
.196						.196 (.197-.198)
.200					.200 (.201-.206)	.200 (.201-.202)
.204						.204 (.205-.206)
.208				.208 (.209-.222)	.208 (.209-.214)	.208 (.209-.210)
.212						.212 (.213-.214)
.216					.216 (.217-.222)	.216 (.217-.218)
.220						.220 (.221-.222)
.224			.224 (.225-.254)	.224 (.225-.238)	.224 (.225-.230)	.224 (.225-.226)
.228						.228 (.229-.230)
.232					.232 (.233-.238)	.232 (.233-.234)
.236						.236 (.237-.238)
.240				.240 (.241-.254)	.240 (.241-.246)	.240 (.241-.242)
.244						.244 (.245-.246)
.248					.248 (.249-.254)	.248 (.249-.250)
.252						.252 (.253-.254)

Figure 188. Elección de bloques para las WAN aplicando cuadro VLSM

/25 (subred de 1 bit) subred de 2 bits 126 hosts		/26 (subred de 2 bits) 4 máscaras de subred	/27 (subred de 3 bits) 8 subredes 30 hosts	/28 (subred de 4 bits) 16 subredes 14 hosts	/29 (subred de 5 bits) 32 subredes 6 hosts	/30 (subred de 6 bits) 64 subredes 2 hosts
.128	Dirección asignada			.128 (.129-.142)	.128 (.129-.134)	.128 (.129-.130)
.132						.132 (.133-.134)
.136					.136 (.137-.142)	.136 (.137-.138)
.140						.140 (.141-.142)
.144	.128	.128 (.129-.190)	.128 (.129-.158)	.144 (.145-.158)	.144 (.145-.150)	.144 (.145-.146)
.148						.148 (.149-.150)
.152					.152 (.153-.158)	.152 (.153-.154)
.156						.156 (.157-.158)
.160			.160 (.161-.190)	.160 (.161- 174)	.160 (.161-.166)	.160 (.161-.162)
.164						.164 (.165-.166)
.168					.168 (.169-.174)	.168 (.169-.170)
.172						.172 (.173-.174)
.176				.176 (.177-.190)	.176 (.177-.182)	.176 (.177-.178)
.180						.180 (.181-.182)
.184					.184 (.185-.190)	.184 (.185-.186)
.188						.188 (.189-.190)
.192		.192 (.193-.254)	.192 (.193-.222)	.192 (.193-.206)	.192 (.193-.202)	.192 (.193-.194)
.196						.196 (.197-.198)
.200					.200 (.201-.206)	.200 (.201-.202)
.204						.204 (.205-.206)
.208				.208 (.209-.222)	.208 (.209-.214)	.208 (.209-.210)
.212						.212 (.213-.214)
.216					.216 (.217-.222)	.216 (.217-.218)
.220						.220 (.221-.222)
.224			.224 (.225-.254)	.224 (.225-.238)	.224 (.225-.230)	.224 (.225-.226)
.228						.228 (.229-.230)
.232					.232 (.233-.238)	.232 (.233-.234)
.236						.236 (.237-.238)
.240				.240 (.241-.254)	.240 (.241-.246)	.240 (.241-.242)
.244						.244 (.245-.246)
.248					.248 (.249-.254)	.248 (.249-.250)
.252						.252 (.253-.254)

Figure 189. Elección de bloques para las WAN aplicando cuadro VLSM

Como se ha podido observar, el uso de VLSM permite maximizar el direccionamiento y minimizar el desperdicio. El método del cuadro que se mostró es apenas otra herramienta que los administradores y técnicos de red pueden usar para crear un esquema de direccionamiento que ocasione menos desperdicio que el enfoque de bloques de tamaño fijos.

Ejercicios para practica de estudiante

La actividad en la siguiente ilustración ofrece práctica para la determinación de direcciones de red. Se presentarán máscaras y direcciones host aleatorias. Para cada par de máscaras y direcciones host.

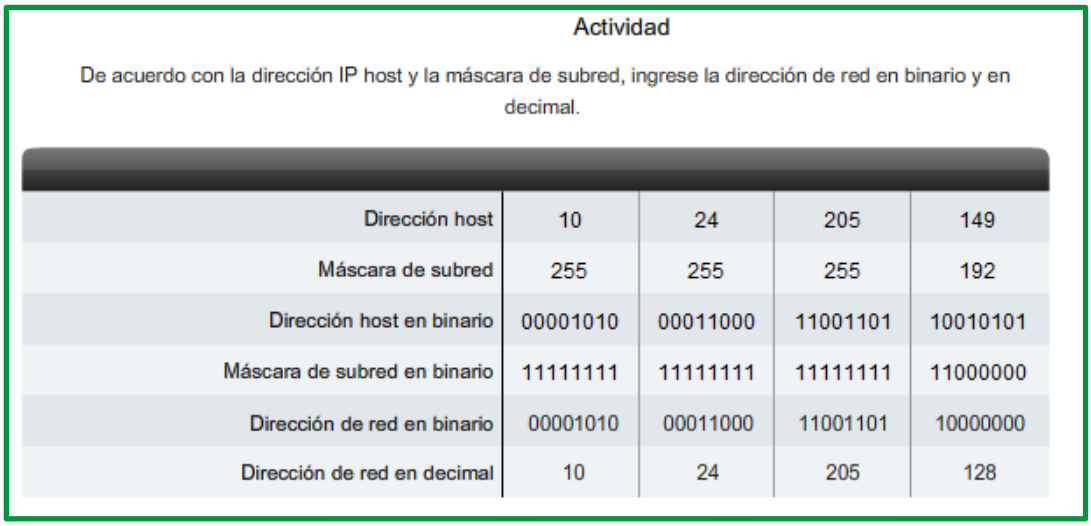


Figure 190. Actividad relacionada con la IP host 10.24.20.149/26

La actividad en la siguiente ilustración ofrece práctica para determinar la cantidad máxima de hosts para una red. Se presentarán máscaras y direcciones host aleatorias. Para cada par de máscaras y direcciones host se ingresa la cantidad máxima de hosts para la red descrita.

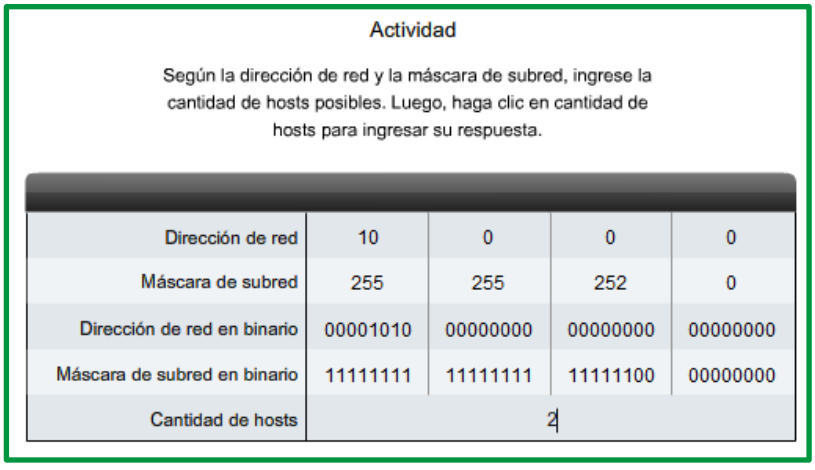


Figure 191. Actividad relacionada con la red 10.0.0.0/22

La actividad en la siguiente ilustración ofrece práctica para determinar direcciones hosts, de red y de broadcast para una red. Se presentarán máscaras y direcciones host aleatorias. Para cada par de máscaras y direcciones host se deberá ingresar direcciones hosts, de red y de broadcast.

Actividad

Dadas la dirección de red y la máscara de subred, defina el rango de hosts, la dirección de broadcast y la siguiente dirección de red. Haga clic en el octeto de la tabla para ingresar la información.

Dirección de red en formato decimal	10	254	128	0
Máscara de subred en formato decimal	255	255	224	0
Dirección de red en formato binario	00001010	11111110	10000000	00000000
Máscara de subred en formato binario	11111111	11111111	11100000	00000000
Primer dirección IP de host utilizable en formato decimal	10	254	128	1
Última dirección IP de host utilizable en formato decimal	10	254	159	254
Dirección de broadcast en formato decimal	10	254	159	255
Siguiente dirección de red en formato decimal	10	254	160	0

Figure 192. Actividad relacionada con la dirección de red 10.254.128.0/19

Establecimiento y medición de rutas estáticas y dinámicas

RUTAS ESTATICAS IPV4

Rutas resumidas

La sumarización de ruta, también conocida como “agregación de rutas”, es el proceso de anunciar un conjunto de direcciones contiguas como una única dirección, con una máscara de subred más corta y menos específica. CIDR es una forma de sumarización de ruta y es un sinónimo del término “creación de superredes”.

CIDR omite la restricción de límites con clase y permite la sumarización con máscaras más pequeñas que las de la máscara con clase predeterminada. Este tipo de sumarización ayuda a reducir la cantidad de entradas en las actualizaciones de enrutamiento y disminuye la cantidad de entradas en las tablas de enrutamiento locales. Reduce, además, el uso del ancho de banda para las actualizaciones de enrutamiento y acelera las búsquedas en las tablas de enrutamiento.

En la ilustración, el R1 requiere una ruta estática resumida para alcanzar las redes en el rango de 172.20.0.0/16 a 172.23.0.0/16.

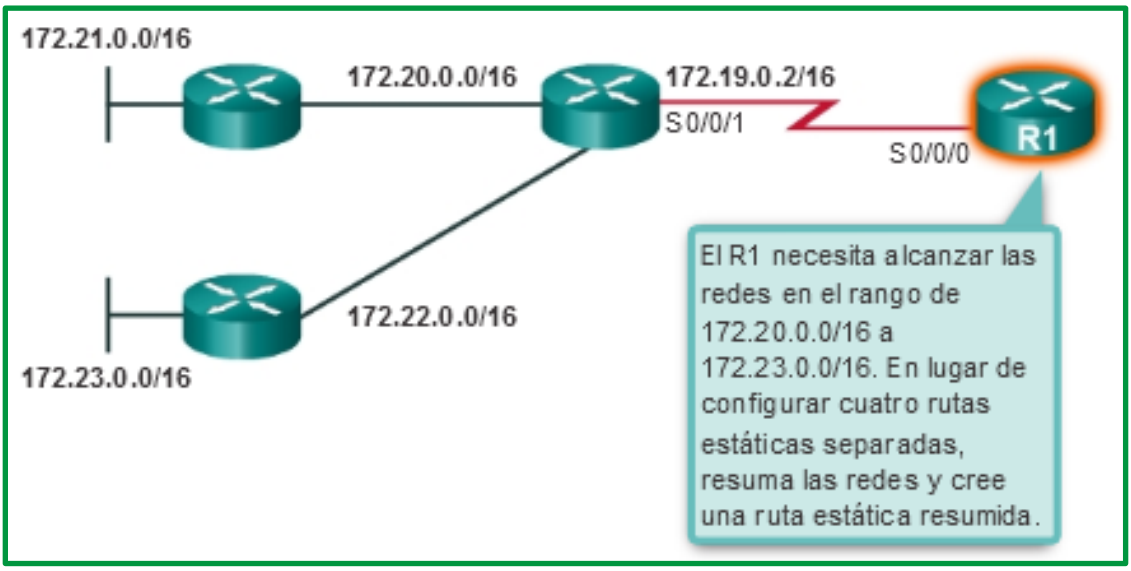


Figure 193. Topología para aplicación de ruta resumida

La sumarización de redes en una única dirección y máscara se puede realizar en tres pasos:

Paso 1. Enumere las redes en formato binario. En la figura siguiente se indican las redes 172.20.0.0/16 a 172.23.0.0/16 en formato binario.

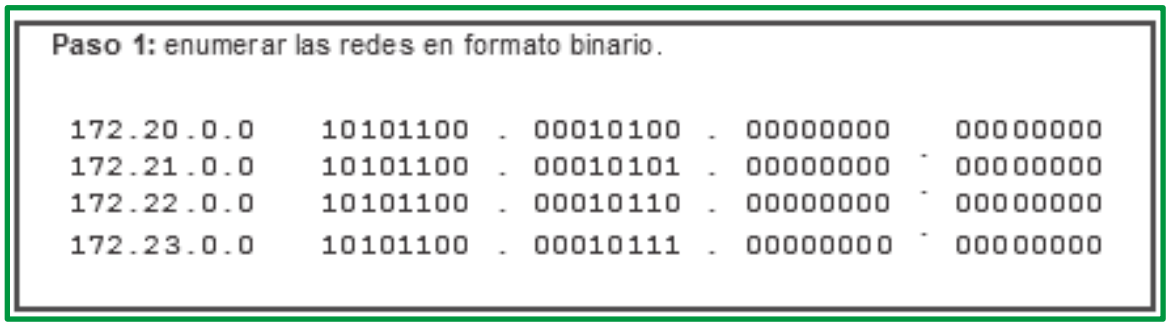


Figure 194. Paso 1

Paso 2. Cuente el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la máscara de la ruta resumida. En la figura 2, se destacan los 14 bits coincidentes que se encuentran en el extremo izquierdo. Este es el prefijo, o la máscara de subred, para la ruta resumida: /14 o 255.252.0.0.

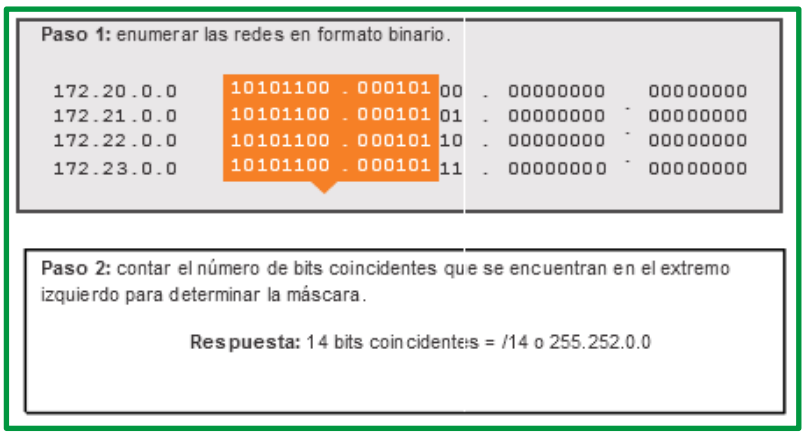


Figure 195. Paso 2

Paso 3. Copie los bits coincidentes y luego agregue los bits 0 para determinar la dirección de red resumida. En la figura 3, se muestra que los bits coincidentes con ceros al final producen la dirección de red 172.20.0.0. Las cuatro redes (172.20.0.0/16, 172.21.0.0/16, 172.22.0.0/16 y 172.23.0.0/16) pueden sumarizar en una única dirección de red y prefijo 172.20.0.0/14.

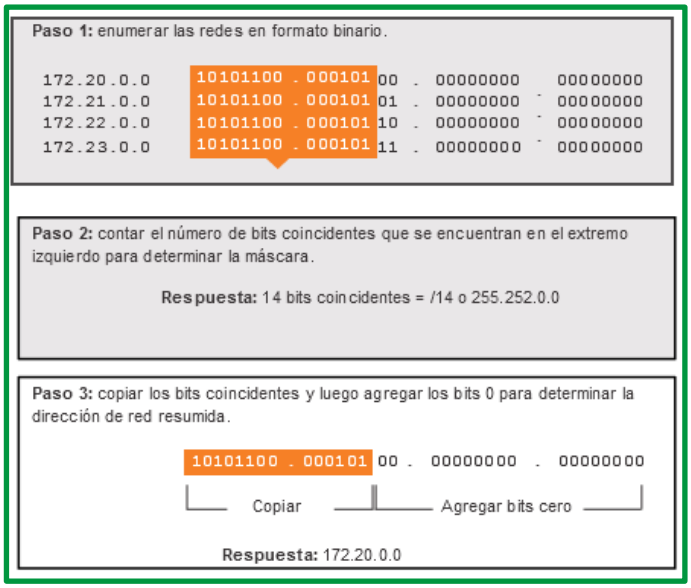


Figure 196. Paso 3

En la figura siguiente, se muestra el R1 configurado con una ruta estática resumida para alcanzar las redes 172.20.0.0/16 a 172.23.0.0/16.

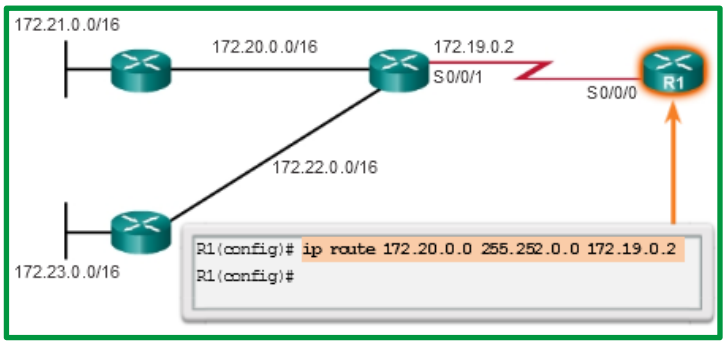


Figure 197. Paso 4

Las múltiples rutas estáticas se pueden resumir en una sola ruta estática si:

- Las redes de destino son contiguas y se pueden resumir en una única dirección de red.
- Todas las rutas estáticas utilizan la misma interfaz de salida o la dirección IP del siguiente salto.

Considere el ejemplo de la figura siguiente. Todos los routers tienen conectividad mediante rutas estáticas.

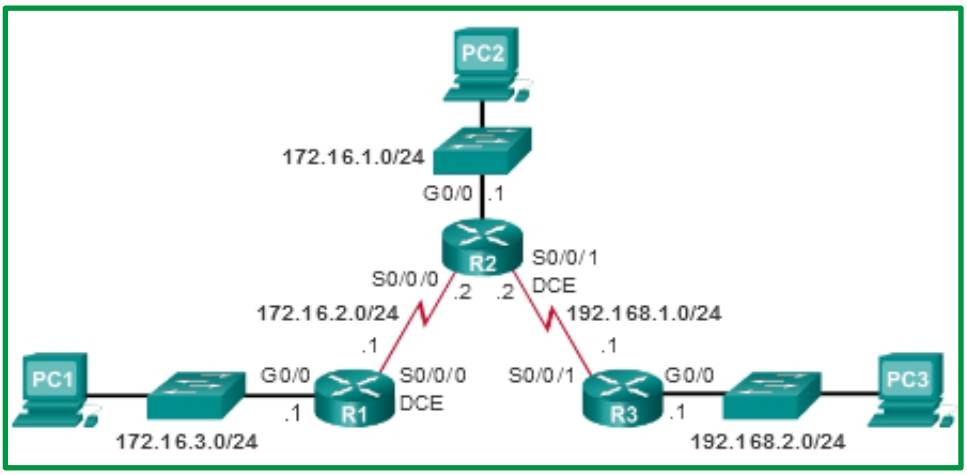


Figure 198. Topología básica

En la figura siguiente, se muestran las entradas de la tabla de routing estático para el R3. Observe que tiene tres rutas estáticas que pueden resumirse, porque comparten los mismos dos primeros octetos.

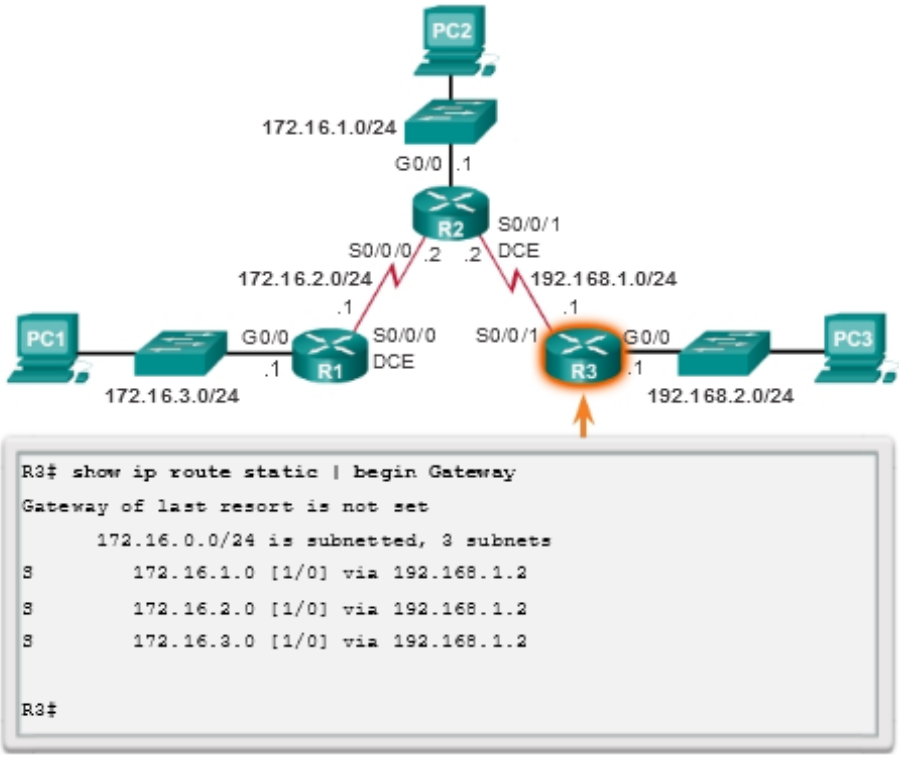


Figure 199. Verificación de tabla de enrutamiento router R3

En la figura siguiente, se muestran los pasos para resumir esas tres redes:

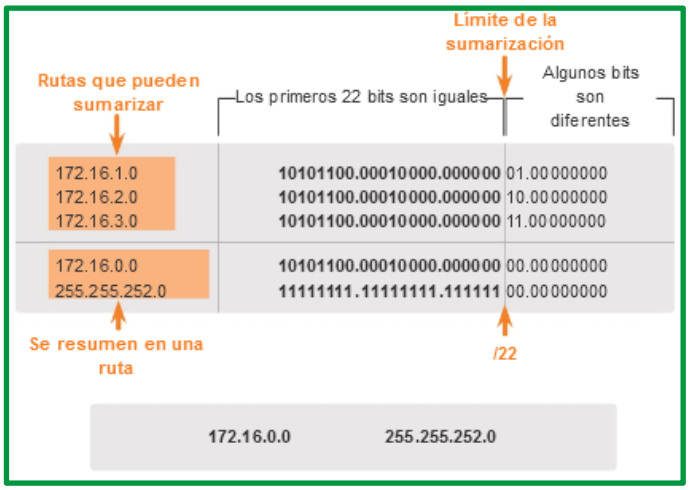


Figure 200. Proceso para resumir rutas

El proceso a seguir se explica a continuación:

- ***Paso 1***. Escriba las redes que se van a resumir en formato binario.
- ***Paso 2***. Para encontrar la máscara de subred para la sumarización, comience con el bit del extremo izquierdo y vaya hacia la derecha. Verá que todos los bits coinciden de forma consecutiva hasta una columna en la cual los bits no coinciden, la cual identifica el límite del resumen.
- ***Paso 3***. Cuente el número de bits coincidentes que se encuentran en el extremo izquierdo. En el ejemplo, es 22. Este número identifica la máscara de subred de la ruta resumida como /22 o 255.255.252.0.
- ***Paso 4***. Para encontrar la dirección de red para el resumen, copie los 22 bits que coinciden y agregue a todos los bits 0 al final para obtener 32 bits.

Después de identificar la ruta resumida, reemplace las rutas existentes por esta ruta.

En la figura siguiente, se muestra cómo se eliminan las tres rutas existentes y, luego, cómo se configura la nueva ruta estática resumida.

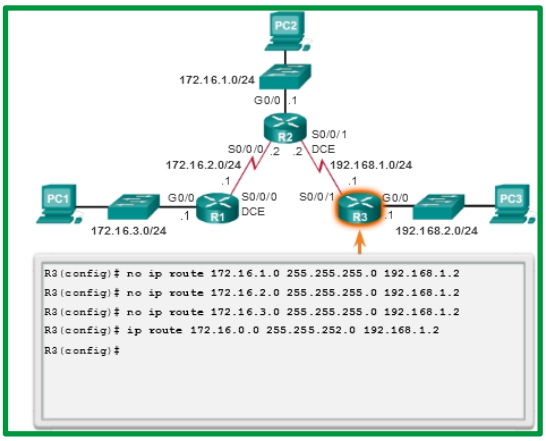


Figure 201. Eliminación de rutas estáticas y configuración de la ruta estática resumida

En la ilustración siguiente se aplica el comando show ip route que muestra que la ruta estática resumida está en la tabla de routing del R3.

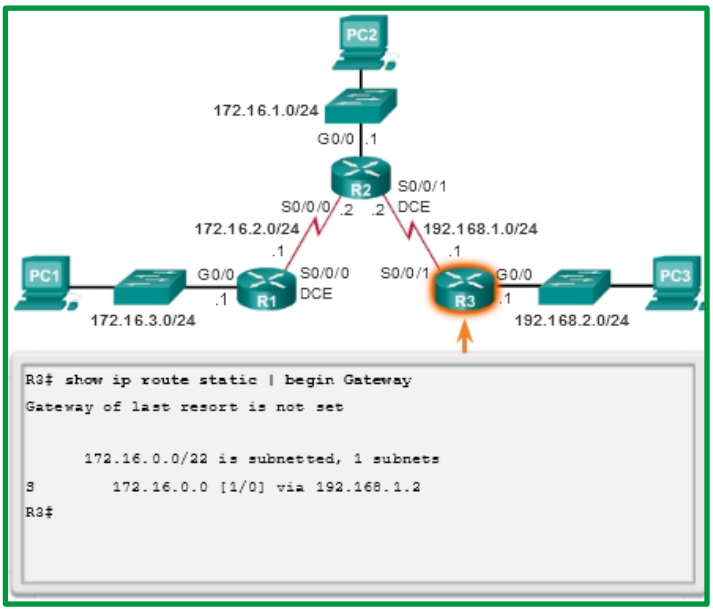


Figure 202. Verificación de ruta estática resumida.

Ejercicios para practica de los estudiantes:

Ejercicio 1: En la ilustración siguiente se muestra topología donde se aplica en R1 una ruta resumida para alcanzar las demás redes, realizar proceso de cálculo binario para resultado obtenido (10.0.0.0/11).

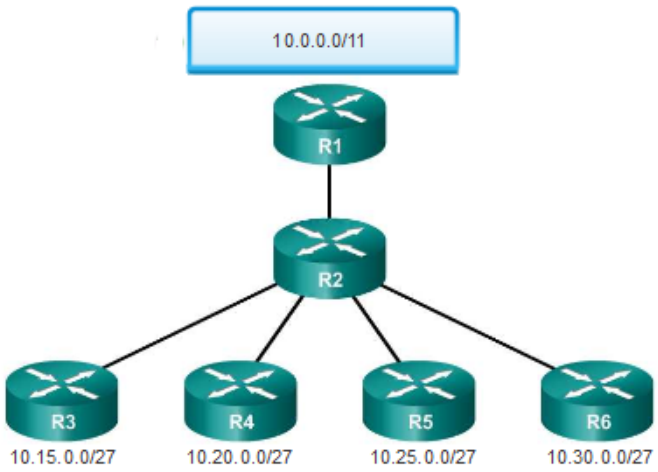


Figure 203. Topología para practica de ruta resumida

Ejercicio 2: En la ilustración siguiente se muestra topología donde R1 necesita alcanzar todas las redes. Determine la ruta resumida para alcanzar las demás redes, realizar proceso de cálculo binario para resultado obtenido.

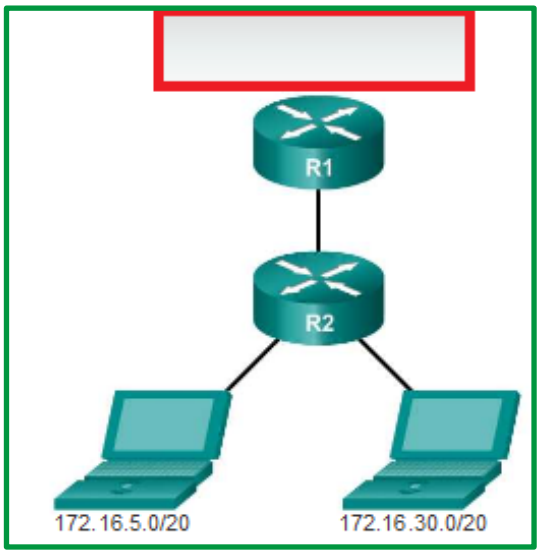


Figure 204. Establezca Ruta resumida para alcanzar todas las redes en R1

Ejercicio 3: En la ilustración siguiente se muestra topología donde R1 necesita alcanzar todas las redes. Determine la ruta resumida para alcanzar las demás redes, realizar proceso de cálculo binario para resultado obtenido.

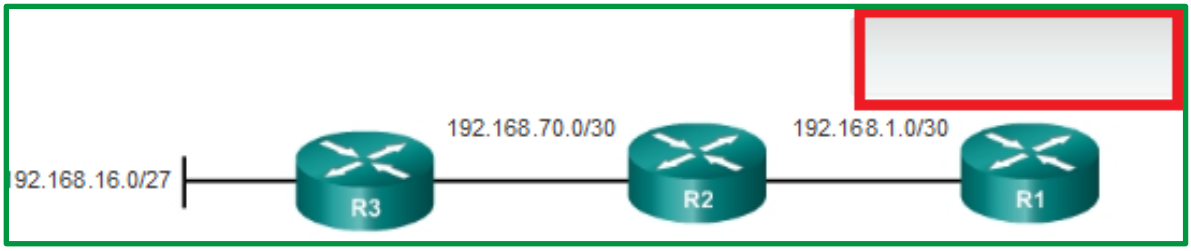


Figure 205. Establezca Ruta resumida para alcanzar todas las redes en R1

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.

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:

- ***ip route*** 0.0.0.0 0.0.0.0 ***{dirección del siguiente salto}***
- ***ip route*** 0.0.0.0 0.0.0.0 ***{interfaz saliente}***

Ejemplo de aplicación:

- ***ip route*** 0.0.0.0 0.0.0.0 ***192.168.1.5***
- ***ip route*** 0.0.0.0 0.0.0.0 ***s0/0/0***

Las ***rutas estáticas flotantes*** son rutas estáticas que tienen una distancia administrativa mayor que la de otra ruta estática o la de rutas dinámicas. Son muy útiles para proporcionar un respaldo a un enlace principal, como se muestra en la ilustración.

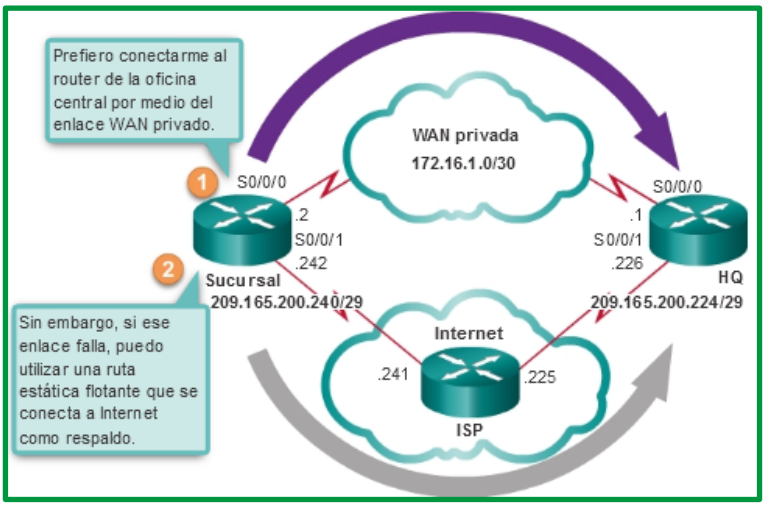


Figure 206. Ruta estática flotante

De manera predeterminada, las rutas estáticas tienen una distancia administrativa de 1, lo que las hace preferibles a las rutas descubiertas mediante protocolos de routing dinámico. Por ejemplo, las distancias administrativas de algunos protocolos de routing dinámico comunes son las siguientes:

- EIGRP = 90
- IGRP = 100
- OSPF = 110
- IS-IS = 115
- RIP = 120

La distancia administrativa de una ruta estática se puede aumentar para hacer que la ruta sea menos deseable que la ruta de otra ruta estática o una ruta descubierta mediante un protocolo de routing dinámico. De esta manera, la ruta estática “flota” y no se utiliza cuando está activa la ruta con la mejor distancia administrativa. Sin embargo, si se pierde la ruta de preferencia, la ruta estática flotante puede tomar el control, y se puede enviar el tráfico a través de esta ruta alternativa.

Una ruta estática flotante se puede utilizar para proporcionar una ruta de respaldo a varias interfaces o redes en un router. También es independiente de la encapsulación, lo que significa que puede utilizarse para reenviar paquetes desde cualquier interfaz, sin importar el tipo de encapsulación.

Es importante tener en cuenta que el tiempo de convergencia afecta una ruta estática flotante. Una ruta que pierde y restablece una conexión de manera continua puede hacer que la interfaz de respaldo se active innecesariamente.

Para configurar rutas estáticas IPv4, se utiliza el comando ip route de configuración global y se especifica una distancia administrativa. Si no se configura ninguna distancia administrativa, se utiliza el valor predeterminado (1).

Consulte la topología en la ilustración. En esta situación, la ruta preferida del R1 es al R2. La conexión al R3 se debe utilizar solo para respaldo.

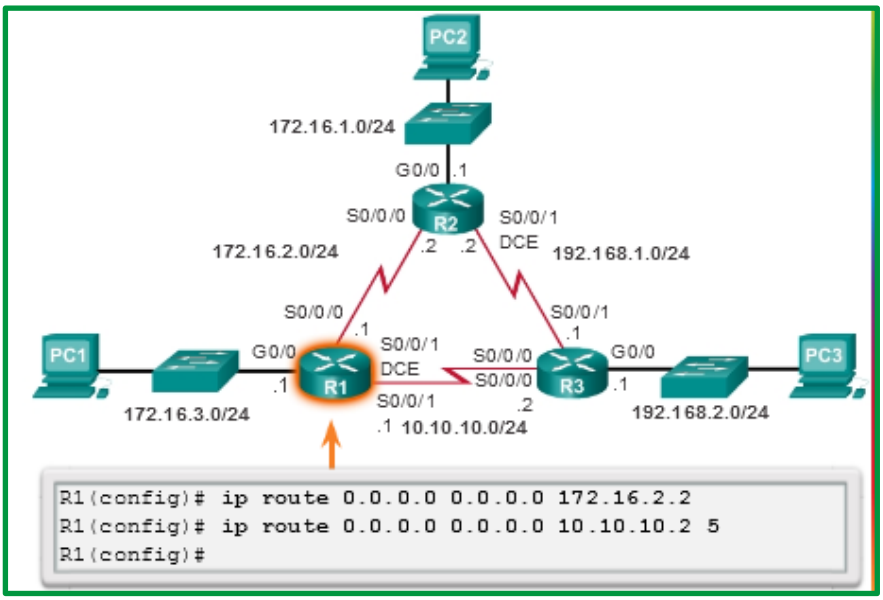


Figure 207. Ruta estática de R1

El R1 se configura con una ruta estática predeterminada que apunte al R2. Debido a que no está configurada ninguna distancia administrativa, se utiliza el valor predeterminado (1) para esta ruta estática. El R1 también está configurado con una ruta estática flotante predeterminada que apunta al R3 con una distancia administrativa de 5. Este valor es mayor que el valor predeterminado 1, y, por lo tanto, esta ruta flota y no está presente en la tabla de routing, a menos que la ruta preferida falle.

En la siguiente ilustración, se verifica que la ruta predeterminada al R2 esté instalada en la tabla de routing. Observe que la ruta de respaldo al R3 no está presente en la tabla de routing.

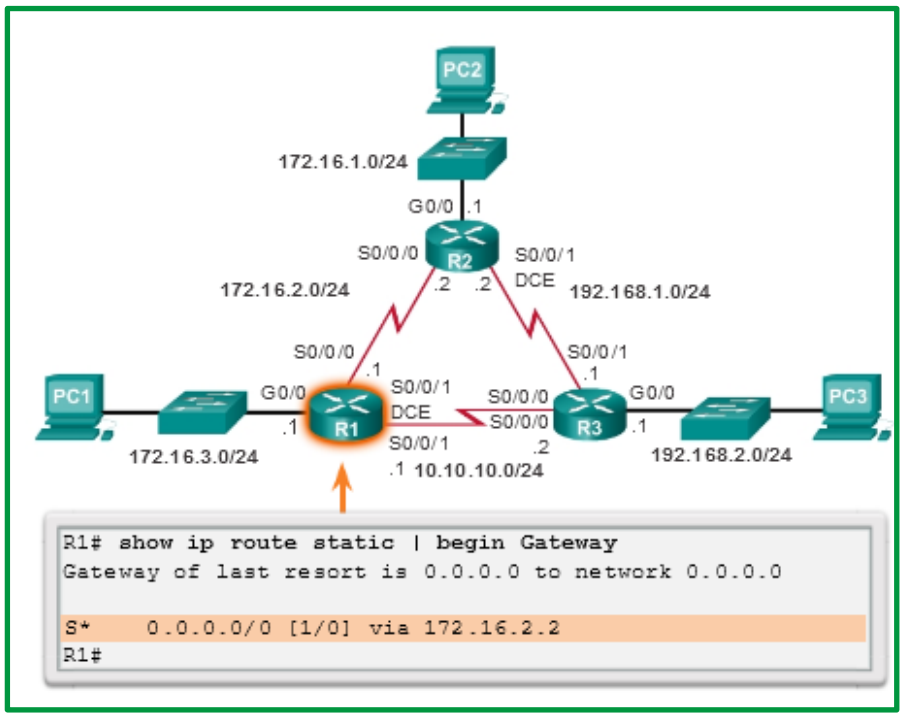


Figure 208. Tabla de enrutamiento de R1

RUTAS RESUMIDAS IPV6

Aparte del hecho de que las direcciones IPv6 tienen una longitud de 128 bits y están escritas en hexadecimales, el resumen de direcciones IPv6 es muy similar al resumen de las direcciones IPv4. Solo requiere de algunos pasos más debido a las direcciones IPv6 abreviadas y a la conversión hexadecimal.

Varias rutas estáticas IPv6 se pueden resumir en una única ruta estática IPv6 si:

- Las redes de destino son contiguas y se pueden resumir en una única dirección de red.
- Todas las rutas estáticas utilizan la misma interfaz de salida o la dirección IPv6 del siguiente salto.

Consulte la red de la ilustración siguiente. Actualmente, el R1 tiene cuatro rutas estáticas IPv6 para alcanzar las redes 2001:DB8:ACAD:1::/64 a 2001:DB8:ACAD:4::/64.

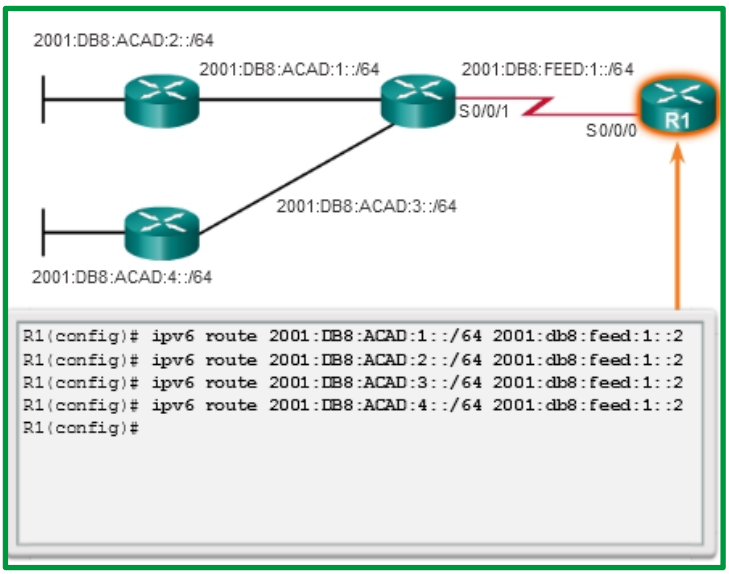


Figure 209. Topología básica para ruta resumida IPv6

El resumen de redes IPv6 en un único prefijo IPv6 y una única longitud de prefijo se puede realizar en siete pasos:

- ***Paso 1***. Enumere las direcciones de red (prefijos) e identifique la parte en la cual las direcciones difieren.

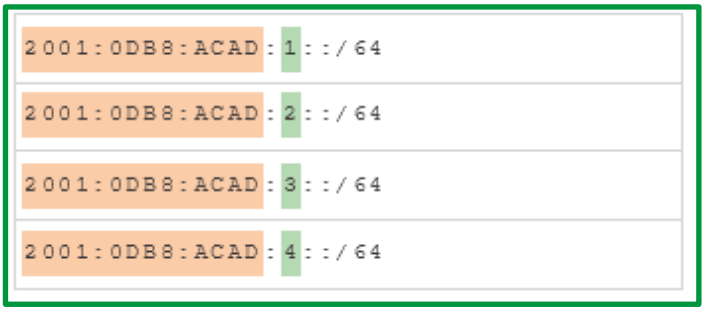


Figure 210. Paso 1

- ***Paso 2***. Expanda la IPv6 si está abreviada.

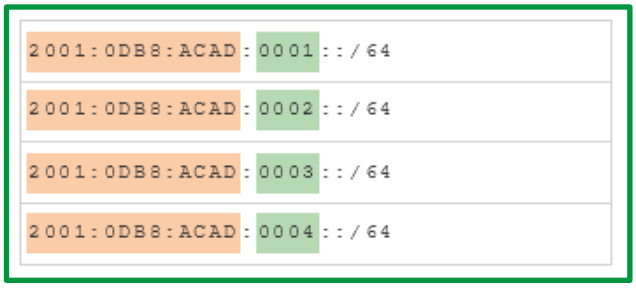


Figure 211. Paso 2

- ***Paso 3***. Convierta la sección diferente de sistema hexadecimal a binario.

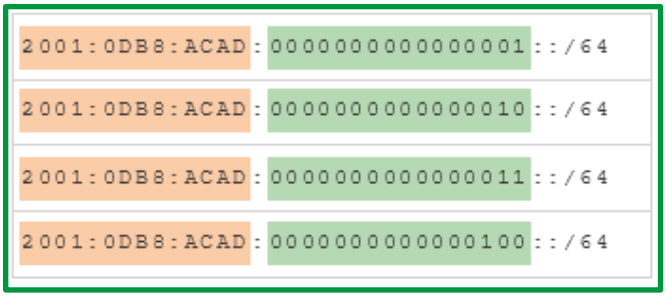


Figure 212. Paso 13

- ***Paso 4***. Cuente el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la longitud de prefijo para la ruta resumida.

Figure 213. Paso 4

- ***Paso 5***. Copie los bits coincidentes y luego agregue los bits 0 para determinar la dirección de red resumida (prefijo).

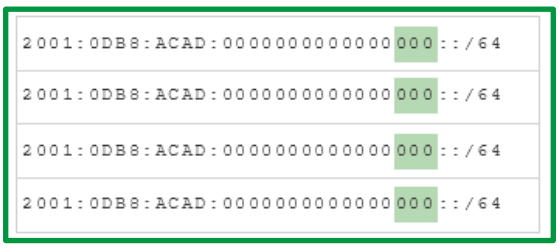


Figure 214. Paso 15

- ***Paso 6***. Convierta la sección binaria de nuevo en hexadecimal.

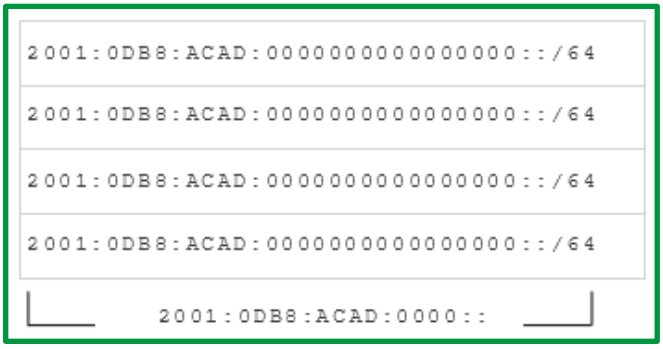


Figure 215. Paso 6

- ***Paso 7***. Agregue el prefijo de la ruta resumida (resultado del paso 4).

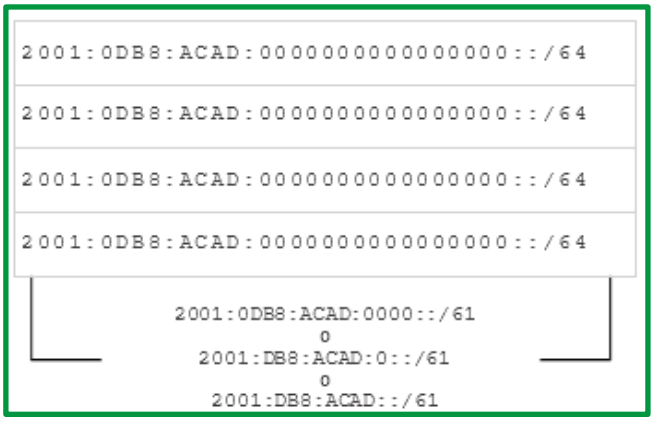


Figure 216. Paso 7

Después de identificar la ruta resumida, reemplace las rutas existentes por esta ruta.

En la ilustración siguiente, se muestra cómo se eliminan las cuatro rutas existentes y, luego, cómo se configura la nueva ruta estática resumida IPv6.

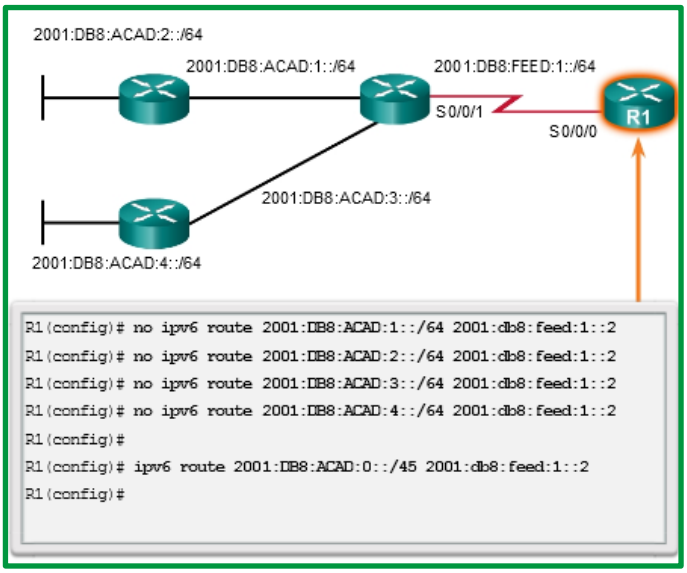


Figure 217. Eliminación de rutas existente y agregar ruta resumida (IPv6)

RUTAS DINAMICAS.

Un router con encaminamiento dinámico; es capaz de entender la red y pasar las rutas entre routers vecinos. Con esto puede señalar que es la propia red gracias a los routers con routing dinámico los que al agregar nuevos nodos o perderse algún enlace es capaz de poner/quitar la ruta del nodo en cuestión en la tabla de rutas del resto de la red o de buscar un camino alternativo o más óptimo en caso que fuese posible.

Los protocolos de enrutamiento se usan para facilitar el intercambio de información de enrutamiento entre los routers. Un protocolo de enrutamiento es un conjunto de procesos, algoritmos y mensajes que se usan para intercambiar información de enrutamiento y completar la tabla de enrutamiento con la elección de los mejores caminos que realiza el protocolo. El propósito de los protocolos de routing dinámico incluye lo siguiente:

- Descubrir redes remotas
- Mantener la información de enrutamiento actualizada
- Escoger el mejor camino hacia las redes de destino
- Poder encontrar un mejor camino nuevo si la ruta actual deja de estar disponible

Los componentes principales de los protocolos de routing dinámico incluyen los siguientes:

- ***Estructuras de datos***: por lo general, los protocolos de routing utilizan tablas o bases de datos para sus operaciones. Esta información se guarda en la RAM.
- ***Mensajes del protocolo de routing***: los protocolos de routing usan varios tipos de mensajes para descubrir routers vecinos, intercambiar información de routing y realizar otras tareas para descubrir la red y conservar información precisa acerca de ella.
- ***Algoritmo***: un algoritmo es una lista finita de pasos que se usan para llevar a cabo una tarea. Los protocolos de enrutamiento usan algoritmos para facilitar información de enrutamiento y para determinar el mejor camino.

En general, las operaciones de un protocolo de enrutamiento dinámico pueden describirse de la siguiente manera:

1. El router envía y recibe mensajes de enrutamiento en sus interfaces.

2. El router comparte mensajes de enrutamiento e información de enrutamiento con otros routers que están usando el mismo protocolo de enrutamiento.

3. Los routers intercambian información de enrutamiento para obtener información sobre redes remotas.

4. Cuando un router detecta un cambio de topología, el protocolo de enrutamiento puede anunciar este cambio a otros routers.

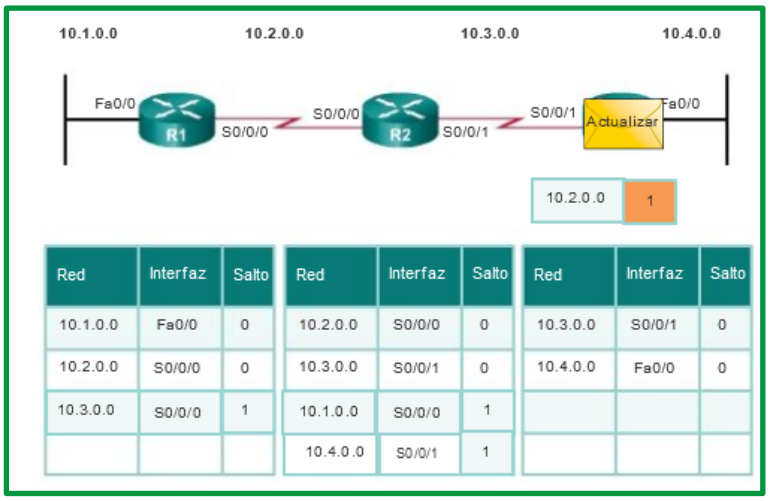


Figure 218. Proceso de actualización automático de tabla de enrutamiento

Los protocolos de enrutamiento se pueden clasificar en diferentes grupos según sus características. Específicamente, los protocolos de routing se pueden clasificar según lo siguiente:

Propósito: protocolo de gateway interior (IGP) o protocolo de gateway exterior (EGP)

Operación: vector distancia, protocolo de estado de enlace, protocolo vector ruta

Comportamiento: protocolo con clase (antiguo) o protocolo sin clase

Por ejemplo, los protocolos de routing IPv4 se clasifican de la siguiente manera:

- RIPv1 (antiguo): IGP, vector distancia, protocolo con clase
- IGRP (antiguo): IGP, vector distancia, protocolo con clase desarrollado por Cisco (cayó en desuso a partir del IOS 12.2)
- RIPv2: IGP, vector distancia, protocolo sin clase
- EIGRP: IGP, vector distancia, protocolo sin clase desarrollado por Cisco
- OSPF: IGP, estado de enlace, protocolo sin clase
- IS-IS: IGP, estado de enlace, protocolo sin clase
- BGP: EGP, vector ruta, protocolo sin clase

Análisis de una tabla de routing IPv4

La topología que se muestra en la figura se utiliza como la topología de referencia para esta sección. Observe lo siguiente en la topología:

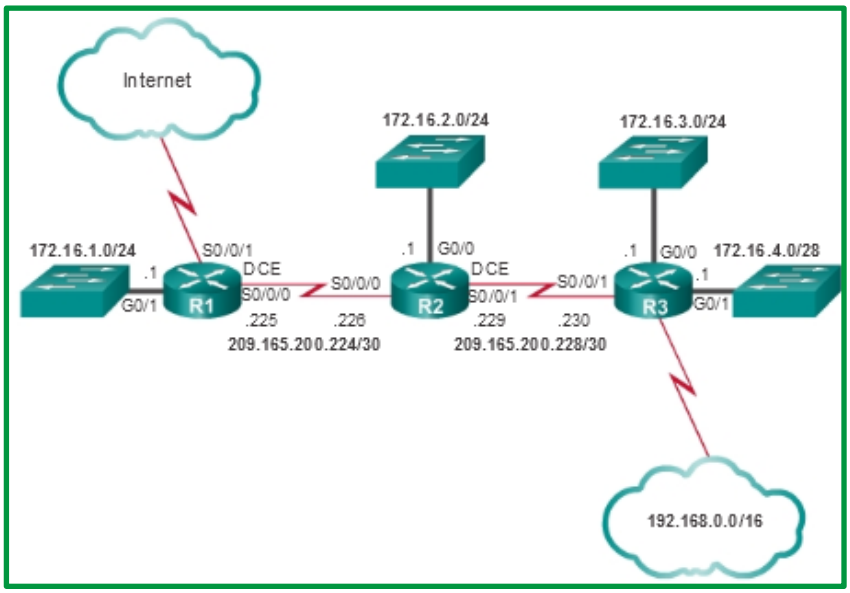


Figure 219. Topología de referencia

- El R1 es el router perimetral que se conecta a Internet. Por lo tanto, propaga una ruta estática predeterminada al R2 y al R3.
- El R1, el R2 y el R3 contienen redes no contiguas separadas por otra red con clase.
- El R3 también introduce una ruta de superred 192.168.0.0/16.

En la siguiente ilustración, se muestra la tabla de routing IPv4 del R1 con las rutas dinámicas, estáticas y conectadas directamente.

```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network 0.0.0.0

S*  0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
                    is directly connected, Serial0/0/1
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C        172.16.1.0/24 is directly connected, GigabitEthernet0/0
L        172.16.1.1/32 is directly connected, GigabitEthernet0/0
R        172.16.2.0/24 [120/1] via 209.165.200.226,00:00:12,
         Serial0/0/0
R        172.16.3.0/24 [120/2] via 209.165.200.226, 00:00:12,
         Serial0/0/0
R        172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:12,
         Serial0/0/0
R        192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03,
         Serial0/0/0
      209.165.200.0/24 is variably subnetted, 5 subnets, 2 masks
C        209.165.200.224/30 is directly connected, Serial0/0/0
L        209.165.200.225/32 is directly connected, Serial0/0/0
R        209.165.200.228/30 [120/1] via 209.165.200.226, 00:00:12,
         Serial0/0/0
C        209.165.200.232/30 is directly connected, Serial0/0/1
L        209.165.200.233/32 is directly connected, Serial0/0/1
R1#
```

Figure 220. Tabla de enrutamiento de router R1

Como se destaca en la ilustración, la tabla de routing del R1 contiene tres redes conectadas directamente. Observe que cuando se configura una interfaz del router activa con una dirección IP y una máscara de subred, automáticamente se crean dos entradas en la tabla de routing.

En la figura siguiente, se muestra una de las entradas de la tabla de routing en el R1 para la red conectada directamente 172.16.1.0. Estas entradas se agregaron de forma automática a la tabla

de enrutamiento cuando se configuró y se activó la interfaz GigabitEthernet 0/0. Las entradas contienen la siguiente información:

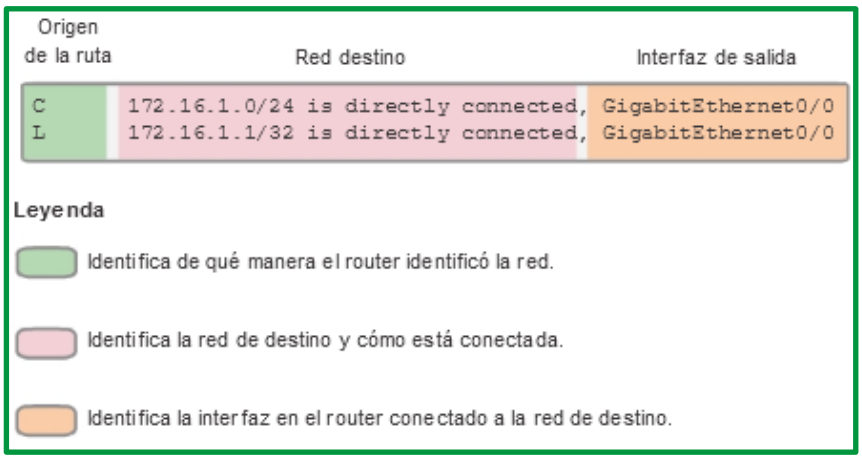


Figure 221. Entradas de la tabla de routing en el R1 para la red conectada directamente 172.16.1.0

Origen de la ruta: identifica el modo en que se descubrió la ruta. Las interfaces conectadas directamente tienen dos códigos de origen de ruta. ***C*** identifica una red conectada directamente. Las redes conectadas directamente se crean de forma automática cada vez que se configura una interfaz con una dirección IP y se activa. ***L*** identifica que la ruta es local. Las rutas locales se crean de forma automática cada vez que se configura una interfaz con una dirección IP y se activa.

Red de destino: la dirección de la red remota y la forma en que se conecta esa red.

Interfaz de salida: identifica la interfaz de salida que se utiliza para reenviar paquetes a la red de destino.

En general, los routers tienen varias interfaces configuradas. En la tabla de routing se almacena información acerca de las rutas conectadas directamente y de las rutas remotas. Tal como ocurre con las redes conectadas directamente, el origen de la ruta identifica cómo se descubrió la ruta. Por ejemplo, los códigos frecuentes para las redes remotas incluyen los siguientes:

- **S**: indica que un administrador creó la ruta manualmente para llegar a una red específica. Esto se conoce como “ruta estática”.
- **D**: indica que la ruta se descubrió de forma dinámica de otro router mediante el protocolo de routing EIGRP.
- **O**: indica que la ruta se descubrió de forma dinámica de otro router mediante el protocolo de routing OSPF.
- **R**: indica que la ruta se descubrió de forma dinámica de otro router mediante el protocolo de routing RIP.

En la ilustración, se muestra una entrada de la tabla de routing IPv4 en el R1 para la ruta hacia la red remota 172.16.4.0 en el R3.

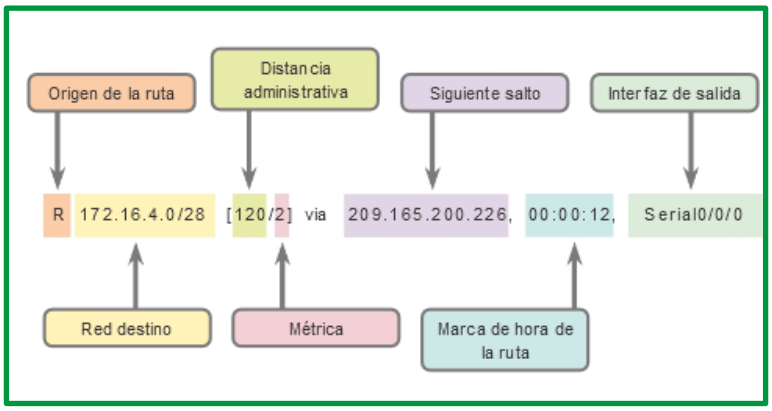


Figure 222. Entrada de la tabla de enrutamiento de R1

La entrada indica la siguiente información:

- **Origen de la ruta:** Identifica el modo en que se descubrió la ruta**.**
- **Red de destino:** Identifica la dirección de la red remota**.**
- **Distancia administrativa:** Identifica la confiabilidad del origen de la ruta**.**
- **Métrica:** Identifica el valor asignado para llegar a la red remota. Los valores más bajos indican las rutas preferidas.
- **Siguiente salto:** Identifica la dirección IPv4 del router siguiente al que se debe reenviar el paquete.
- **Marca de hora de la ruta:** Identifica cuándo fue la última comunicación con la ruta**.**
- **Interfaz de salida:** Identifica la interfaz de salida que se debe utilizar para reenviar un paquete hacia el destino final.

Ejercicio de tabla de enrutamiento: Dada la siguiente tabla de enrutamiento en la ilustración siguiente, determine la ruta, origen de la ruta, distancia administrativa y métrica analizando la tabla de enrutamiento.

```
Gateway of last resort is not set

   10.0.0.0/16 is subnetted, 1 subnets
S     10.4.0.0 is directly connected, Serial0/0/0
   172.16.0.0/24 is subnetted, 3 subnets
C     172.16.1.0 is directly connected, FastEthernet0/0
C     172.16.2.0 is directly connected, Serial0/0/0
D     172.16.3.0 [90/2172416] via 172.16.2.1, 00:00:18, Serial0/0/0
C  192.168.1.0/24 is directly connected, Serial0/0/1
O  192.168.100.0/24 [110/65] via 172.16.2.1, 00:00:03, Serial0/0/0
O  192.168.110.0/24 [110/65] via 172.16.2.1, 00:00:03, Serial0/0/0
R  192.168.120.0/24 [120/1] via 172.16.2.1, 00:00:18, Serial0/0/0
```

Figure 223. Tabla de enrutamiento para práctica.

Figure 224. Tabla de requerimiento a ser llenada

Figure 225. Resolución de ejercicio propuesto

Las rutas se analizan en términos de lo siguiente:

- **Ruta final**. Una ruta final es una entrada de la tabla de routing que contiene una dirección IPv4 del siguiente salto o una interfaz de salida. Las rutas conectadas directamente, las rutas descubiertas dinámicamente y las rutas locales son rutas finales
- **Ruta de Nivel 1.** Una ruta de nivel 1 con una máscara de subred igual o inferior a la máscara con clase de la dirección de red. Por lo tanto, una ruta de nivel 1 puede ser cualquiera de las siguientes:
    - ***Ruta de red***: Una ruta de red que tiene una máscara de subred igual a la de la máscara con clase.
    - ***Ruta de superred***: Una dirección de red con una máscara menor que la máscara con clase, por ejemplo, una dirección de resumen.
    - ***Ruta predeterminada***: Una ruta estática con la dirección 0.0.0.0/0.

  El origen de la ruta de nivel 1 puede ser una red conectada directamente, una ruta estática o un protocolo de enrutamiento dinámico.

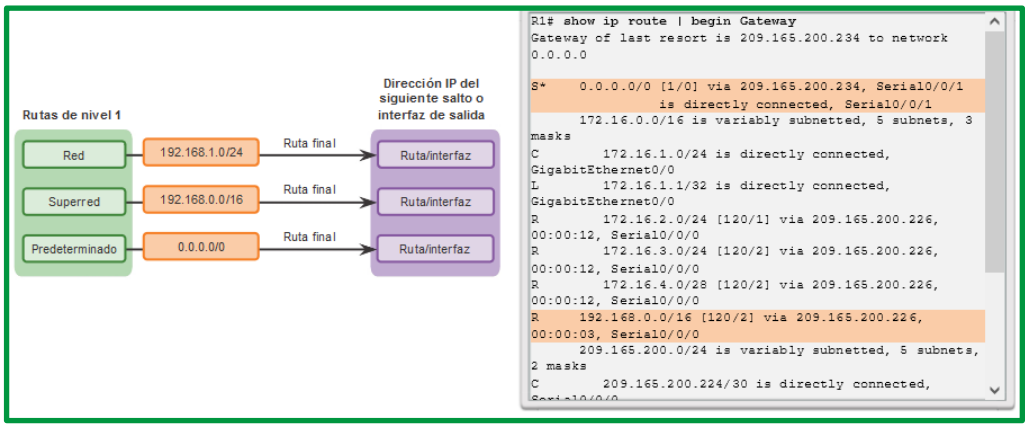


Figure 226. Ruta de nivel 1

- ***Ruta principal de nivel 1***. Una ruta principal de nivel 1 es una ruta de red de nivel 1 que está dividida en subredes. Una ruta principal nunca puede ser una ruta final.

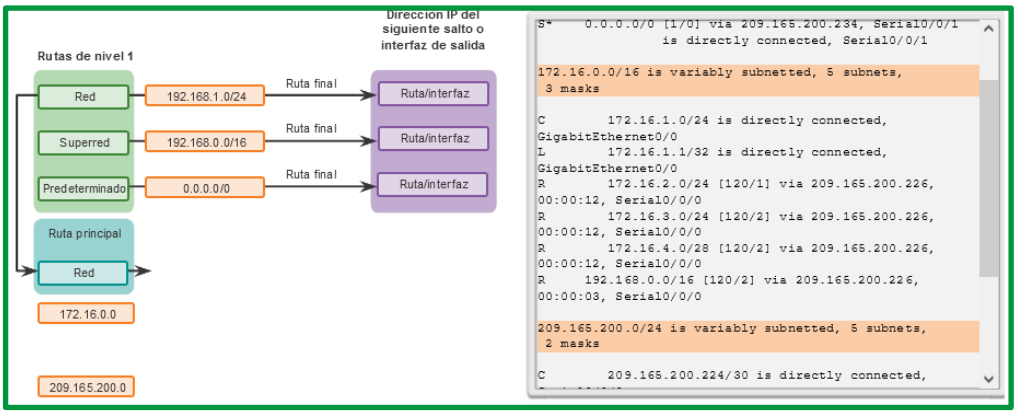


Figure 227. Ruta Principal de nivel 1

- ***Rutas secundarias de nivel 2***. Es una ruta que constituye una subred de una dirección de red con clase. Las rutas principales de nivel 1 contienen rutas secundarias de nivel 2; al igual que en las rutas de nivel 1, el origen de una ruta de nivel 2 puede ser una red conectada directamente, una ruta estática o una ruta descubierta en forma dinámica. Las rutas secundarias de nivel 2 también son rutas finales.

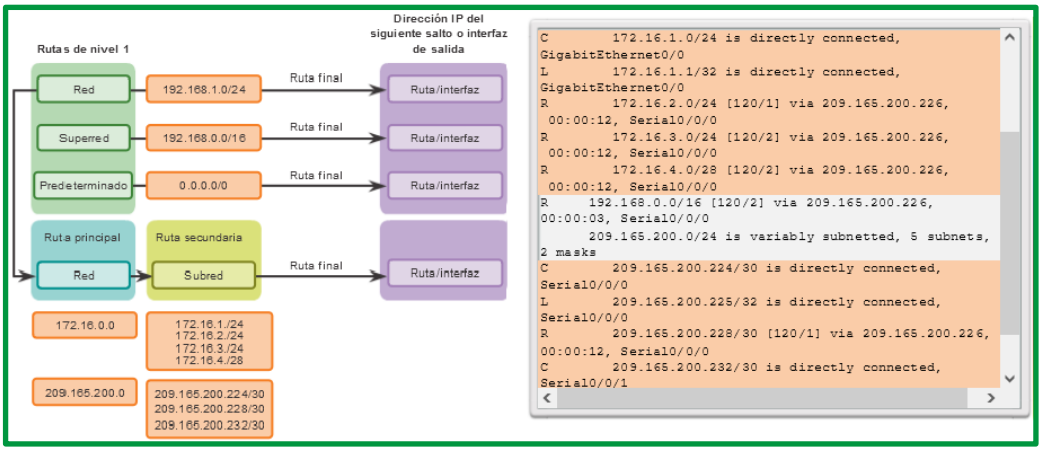


Figure 228. Ruta de nivel 2

Ejercicio de rutas.

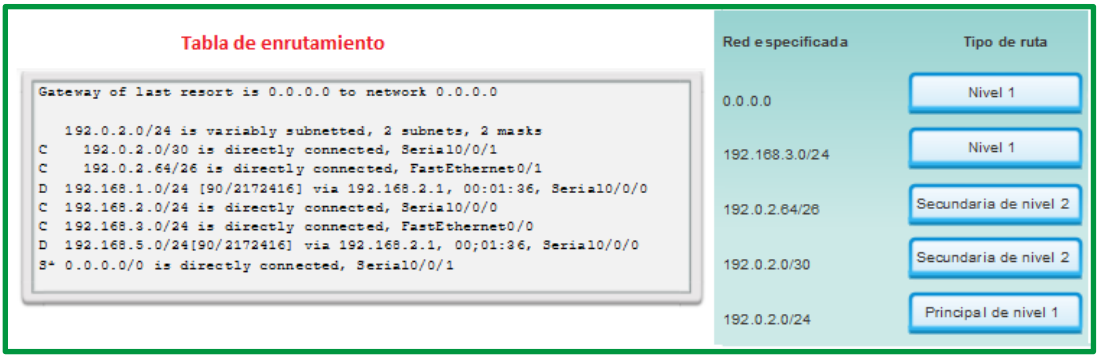


Figure 229. Ejemplo de niveles de ruta a partir de tabla de enrutamiento

Análisis de una tabla de routing IPv6

Los componentes de la tabla de routing IPv6 son muy similares a los de la tabla de routing IPv4. Por ejemplo, se completa con las interfaces conectadas directamente, con las rutas estáticas y con las rutas descubiertas de forma dinámica.

Dado que IPv6 fue diseñado como un protocolo sin clase, todas las rutas son en realidad rutas finales de nivel 1. No hay rutas principales de nivel 1 para rutas secundarias de nivel 2.

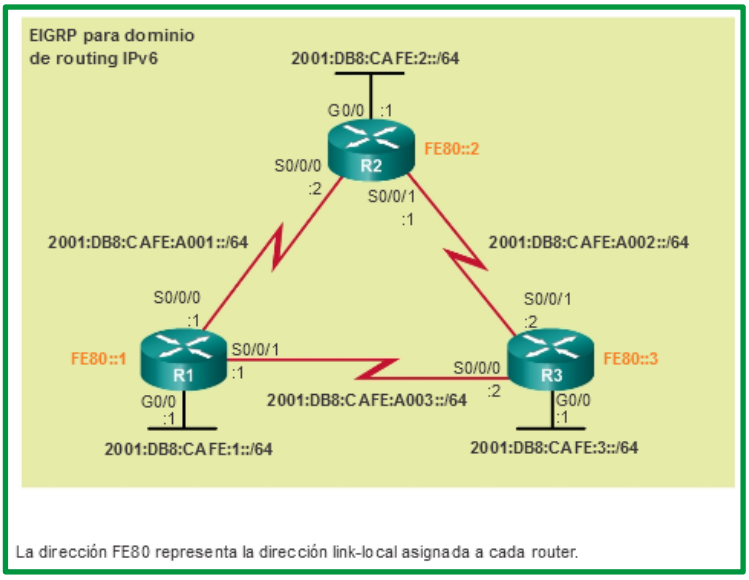


Figure 230. Topología de IPv6 de referencia

La topología que se muestra en la ilustración se utiliza como la topología de referencia para esta sección. Observe lo siguiente en la topología:

- El R1, el R2 y el R3 están configurados en una topología de malla completa. Todos los routers tienen rutas redundantes hacia diversas redes.
- El R2 es el router perimetral y se conecta con el ISP. Sin embargo, no se anuncia una ruta estática predeterminada.
- Se configuró EIGRP para IPv6 en los tres routers.

Como se muestra en la figura siguiente, en las entradas de las rutas conectadas directamente se muestra la siguiente información:

- ***Origen de la ruta***: Identifica el modo en que se descubrió la ruta. Las interfaces conectadas directamente tienen dos códigos de origen de ruta ("C" identifica una red conectada directamente, mientras que "L" identifica que esta es una ruta local).
- ***Red conectada directamente***: La dirección IPv6 de la red conectada directamente.
- ***Distancia administrativa***: Identifica la confiabilidad del origen de la ruta. IPv6 utiliza las mismas distancias que IPv4. El valor 0 indica el mejor origen y el más confiable.
- ***Métrica***: Identifica el valor asignado para llegar a la red remota. Los valores más bajos indican las rutas preferidas.
- ***Interfaz de salida***: Identifica la interfaz de salida que se utiliza para reenviar paquetes a la red de destino.

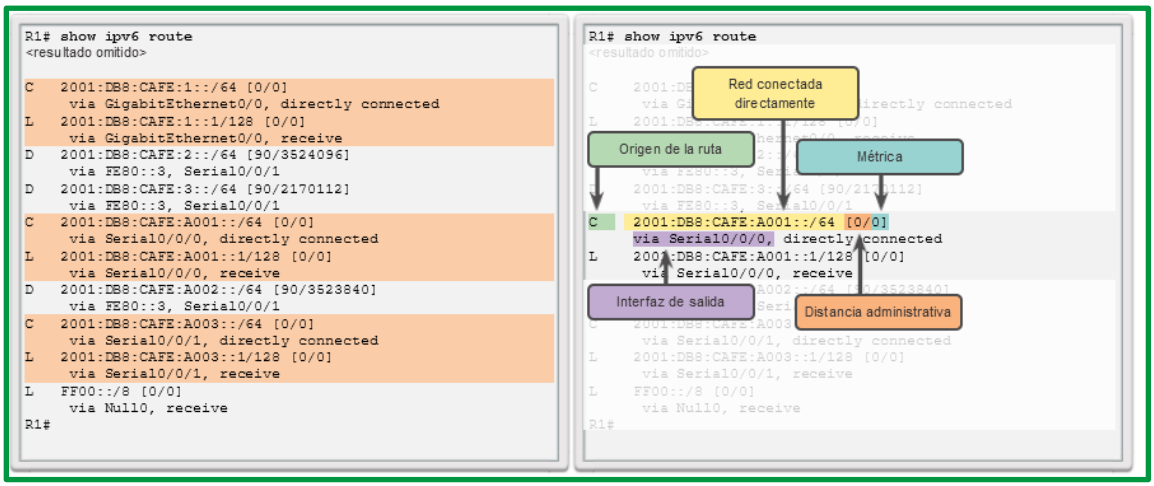


Figure 231. Rutas conectadas directamente a R1

Los enlaces seriales tienen anchos de banda de referencia configurados para observar la forma en que las métricas de EIGRP seleccionan la mejor ruta. El ancho de banda de referencia no es una representación realista de las redes modernas. Se utiliza solamente para proporcionar una idea visual de la velocidad del enlace.

En la figura siguiente, se destacan las entradas de la tabla de routing para las tres redes remotas (es decir, la LAN del R2, la LAN del R3 y el enlace entre el R2 y el R3). Las tres entradas se agregaron mediante EIGRP.

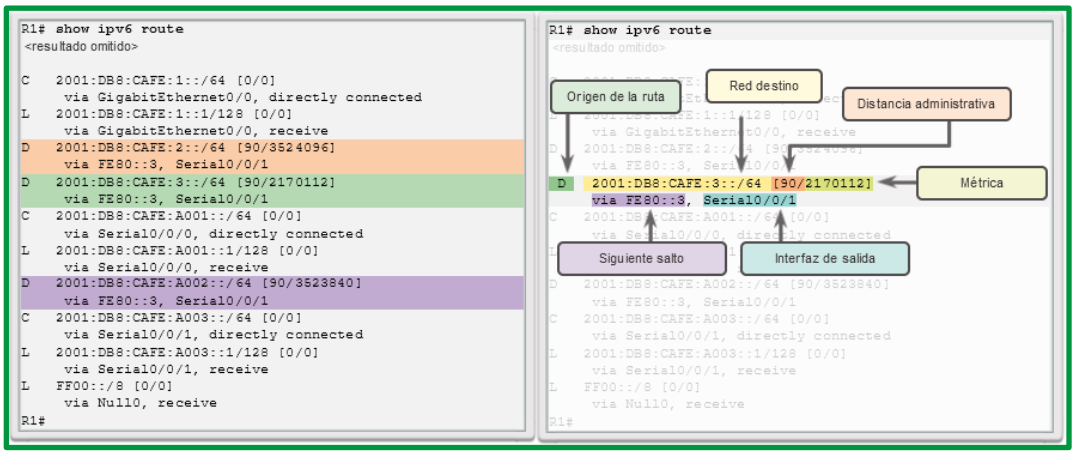


Figure 232. Rutas conectadas remotamente en R1

En la figura se muestra una entrada de la tabla de routing en el R1 para la ruta hacia la red remota 2001:DB8:CAFE:3::/64 en el R3. La entrada indica la siguiente información:

- ***Origen de la ruta***: Identifica el modo en que se descubrió la ruta. Los códigos comunes incluyen O (OSPF), D (EIGRP), R (RIP) y S (ruta estática).
- ***Red de destino***: identifica la dirección de la red IPv6 remota.
- ***Distancia administrativa***: Identifica cuán confiable es el origen de la ruta. IPv6 utiliza las mismas distancias que IPv4.
- ***Métrica***: Identifica el valor asignado para llegar a la red remota. Los valores más bajos indican las rutas preferidas.
- ***Siguiente salto***: Identifica la dirección IPv6 del router siguiente al que se debe reenviar el paquete.
- ***Interfaz de salida***: Identifica la interfaz de salida que se debe utilizar para reenviar un paquete hacia el destino final.

Cuando un paquete IPv6 llega a una interfaz del router, el router analiza el encabezado de IPv6 e identifica la dirección IPv6 de destino. A continuación, el router continúa con el proceso de búsqueda del siguiente router.

El router examina las rutas de red de nivel 1 en busca de la mejor coincidencia con la dirección de destino del paquete IPv6. Al igual que en IPv4, la coincidencia más larga es la mejor coincidencia. Por ejemplo, si hay varias coincidencias en la tabla de routing, el router elige la ruta con la coincidencia más larga. La coincidencia se encuentra entre los bits del extremo izquierdo de la dirección IPv6 de destino del paquete y el prefijo IPv6 y la duración de prefijo en la tabla de routing IPv6.

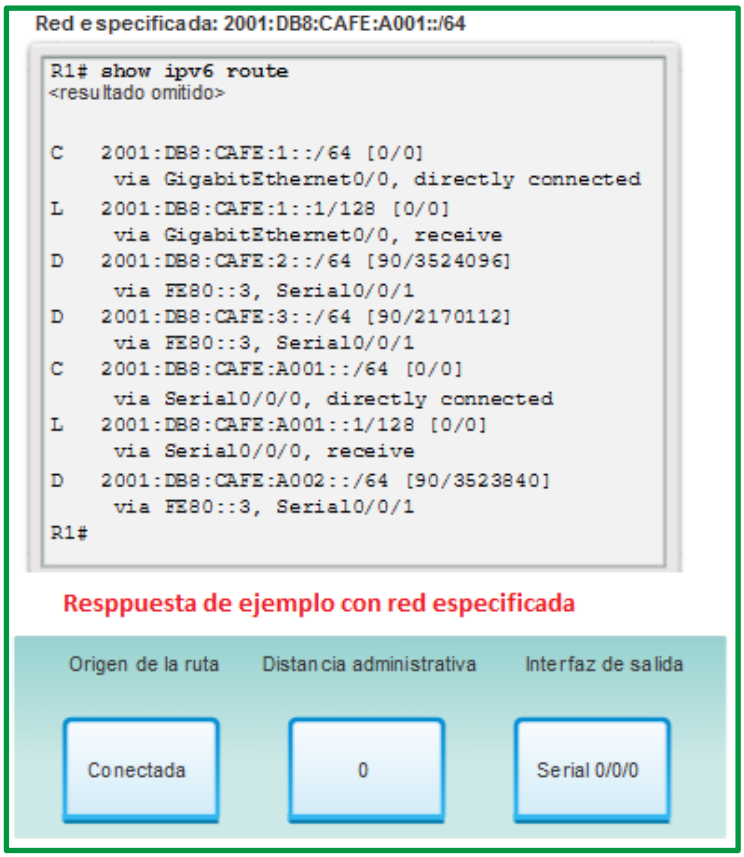


Figure 233. Ejemplo con red especificada 2001:DB8:CAFE:A001::/64

Pruebas en la capa de red

Ping es una utilidad para probar la conectividad IP entre hosts. Ping envía solicitudes de respuestas desde una dirección host específica. Ping usa un protocolo de capa 3 que forma parte del conjunto de aplicaciones TCP/IP llamado Control Message Protocol (Protocolo de mensajes de control de Internet, ICMP). Ping usa un datagrama de solicitud de eco ICMP.

Si el host en la dirección especificada recibe la solicitud de eco, éste responde con un datagrama de respuesta de eco ICMP. En cada paquete enviado, el ping mide el tiempo requerido para la respuesta.

A medida que se recibe cada respuesta, el ping muestra el tiempo entre el envío del ping y la recepción de la respuesta. Ésta es una medida del rendimiento de la red. Ping posee un valor de límite de tiempo de espera para la respuesta. Si no se recibe una respuesta dentro de ese intervalo de tiempo, el ping abandona la comunicación y proporciona un mensaje que indica que no se recibió una respuesta.

Después de enviar todas las peticiones, la utilidad de ping provee un resumen de las respuestas. Este resumen incluye la tasa de éxito y el tiempo promedio del recorrido de ida y vuelta al destino.

Ping del loopback local

Existen casos especiales de prueba y verificación para los cuales se puede usar el ping. Un caso es la prueba de la configuración interna del IP en el host local. Para hacer esta prueba, se realiza el

ping de la dirección reservada especial del loopback local (127.0.0.1), como se muestra en la figura.

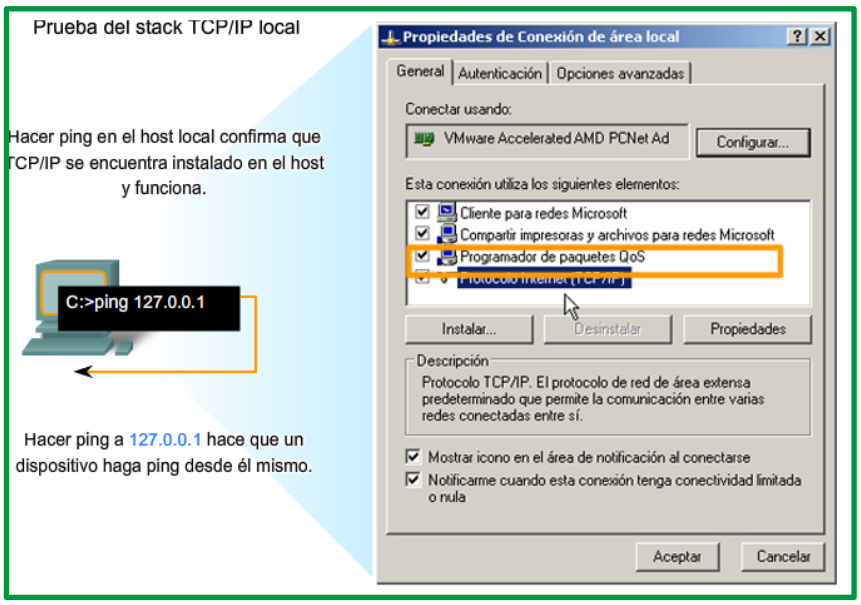


Figure 234. Prueba y verificación de stack TCP/IP

Una respuesta de 127.0.0.1 indica que el IP está correctamente instalado en el host. Esta respuesta proviene de la capa de red. Sin embargo, esta respuesta no indica que las direcciones, máscaras o los gateways estén correctamente configurados. Tampoco indica nada acerca del estado de la capa inferior del stack de red. Sencillamente, prueba la IP en la capa de red del protocolo IP. Si se obtiene un mensaje de error, esto indica que el TCP/IP no funciona en el host.

Ping de Gateway

También es posible utilizar el ping para probar la capacidad de comunicación del host en la red local. Generalmente, esto se hace haciendo ping a la dirección IP del gateway del host, como se muestra en la figura. Un ping en el gateway indica que la interfaz del host y del router que funcionan como gateway funcionan en la red local.

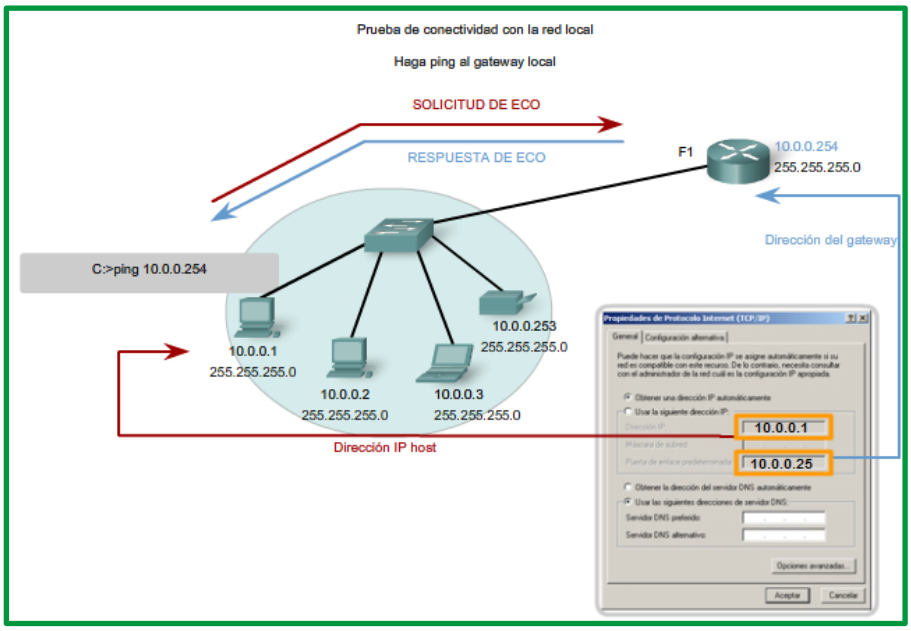


Figure 235. Prueba de conectividad local

Para esta prueba, se usa la dirección de gateway con mayor frecuencia, debido a que el router normalmente está en funcionamiento. Si la dirección de gateway no responde, se puede intentar con la dirección IP de otro host que sepa que funciona en la red local.

Si el gateway u otro host responden, entonces los hosts locales pueden comunicarse con éxito en la red local. Si el gateway no responde, pero otro host sí lo hace, esto podría indicar un problema con la interfaz del router que funciona como gateway.

Una posibilidad es que se tiene la dirección equivocada para el gateway. Otra posibilidad es que la interfaz del router puede estar en funcionamiento, pero se le ha aplicado seguridad, de manera que no procesa o responde a peticiones de ping. También puede suceder que otros hosts tengan la misma restricción de seguridad aplicada.

Ping host remoto

También se puede utilizar el ping para probar la capacidad de comunicación del host IP local en una internetwork. El host local puede hacer ping a un host que funciona en una red remota, como se muestra en la figura.

Si el ping se realiza con éxito, se habrá verificado la operación de una porción amplia de la internetwork. Esto significa que se ha verificado la comunicación del host en la red local, el funcionamiento del router que se usa como gateway y los demás routers que puedan encontrarse en la ruta entre la red y la red del host remoto.

Además, se ha verificado el mismo funcionamiento en el host remoto. Si, por algún motivo, el host remoto no pudo usar su red local para comunicarse fuera de la red, entonces no se habría producido una respuesta.

Recuerde que. - muchos administradores de red limitan o prohíben la entrada de datagramas ICMP en la red corporativa. Por lo tanto, la ausencia de una respuesta de ping podría deberse a restricciones de seguridad y no a elementos que no funcionan en las redes.

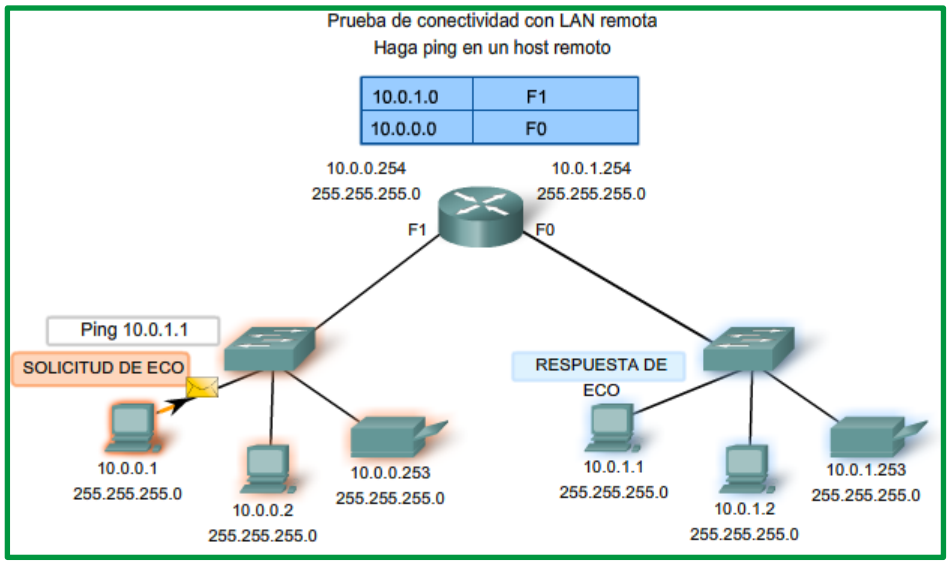


Figure 236. Prueba de conectividad remota

Traceroute (Tracert)

El ping se usa para indicar la conectividad entre dos hosts. Traceroute (tracert) es una utilidad que permite observar la ruta entre estos hosts. El rastreo genera una lista de saltos alcanzados con éxito a lo largo de la ruta.

Esta lista puede suministrar información importante para la verificación y el diagnóstico de fallas. Si los datos llegan a destino, entonces el rastreador menciona la interfaz en cada router que aparece en el camino.

Si los datos fallan en un salto durante el camino, se tiene la dirección del último router que respondió al rastreo. Esto indica el lugar donde se encuentra el problema o las restricciones de seguridad.

Tiempo de ida y vuelta (RTT)

El uso de traceroute proporciona el tiempo de ida y vuelta (RTT) para cada salto a lo largo del camino e indica si se produce una falla en la respuesta del salto. El tiempo de ida y vuelta (RTT) es el tiempo que le lleva a un paquete llegar al host remoto y a la respuesta regresar del host. Se usa un asterisco (*) para indicar la pérdida de un paquete.

Esta información puede ser utilizada para ubicar un router problemático en el camino. Si tenemos altos tiempos de respuesta o pérdidas de datos de un salto particular, ésta es una indicación de que los recursos del router o sus conexiones pueden estar estresados.

Tiempo de vida (TTL)

Traceroute hace uso de una función del campo Tiempo de vida (TTL) en el encabezado de Capa 3 y mensaje excedido en tiempo ICMP. El campo TTL se usa para limitar la cantidad de saltos que un paquete puede cruzar. Cuando un paquete ingresa a un router, el campo TTL disminuye en 1. Cuando el TTL llega a cero, el router no envía el paquete y éste es descartado.

Además de descartar el paquete, el router normalmente envía un mensaje de tiempo superado de ICMP dirigido al host de origen. Este mensaje de ICMP estará conformado por la dirección IP del router que respondió.

La primera secuencia de mensajes enviados desde traceroute tendrá un campo de TTL de uno. Esto hace que el TTL expire el límite de tiempo del paquete en el primer router. Este router luego responde con un mensaje de ICMP. Traceroute ahora posee la dirección del primer salto.

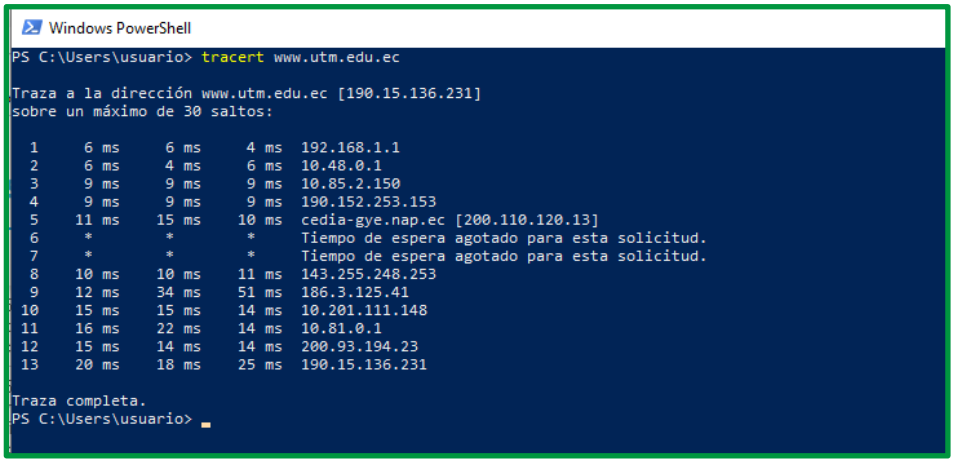


Figure 237. Traza a www.utm.edu.ec

A continuación, Traceroute incrementa progresivamente el campo TTL (2, 3, 4...) para cada secuencia de mensajes. De esta manera se proporciona al rastreo la dirección de cada salto a medida que los paquetes expiran el límite de tiempo a lo largo del camino. El campo TTL continúa aumentando hasta que se llega a destino o hasta un máximo predefinido.

Una vez que se llega al destino final, el host responde con un mensaje de puerto inalcanzable de ICMP o un mensaje de respuesta de eco de ICMP, en lugar del mensaje de tiempo superado de ICMP.

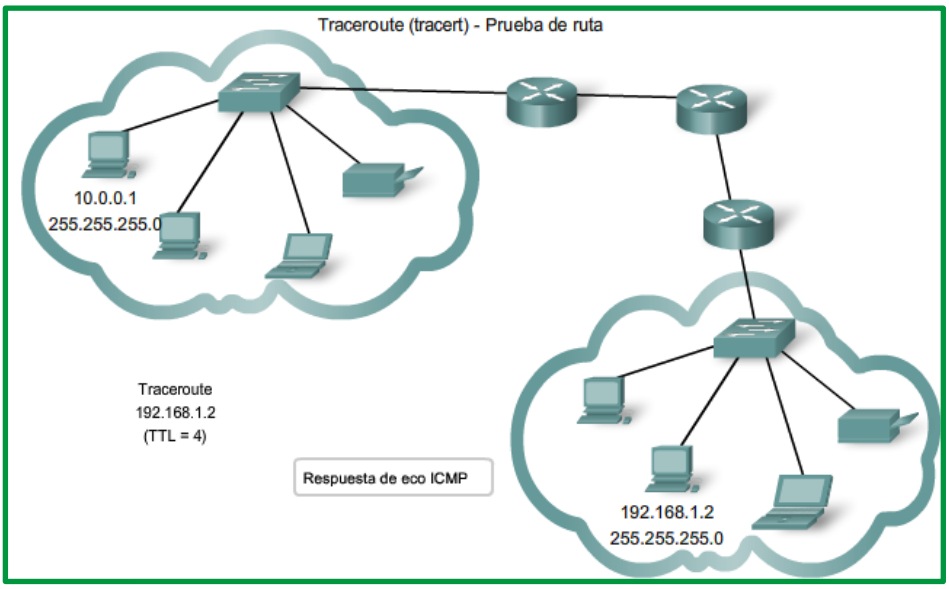


Figure 238. Prueba de ruta aplicando una traza

ICMP

Si bien IP no es un protocolo confiable, la suite TCP/IP proporciona los mensajes que se deben enviar en caso de que se produzcan determinados errores. Estos mensajes se envían mediante los servicios de ICMP. El objetivo de estos mensajes es proporcionar respuestas acerca de temas relacionados con el procesamiento de paquetes IP bajo determinadas condiciones, no es hacer que el IP sea confiable. Los mensajes de ICMP no son obligatorios y, a menudo, no se permiten dentro de una red por razones de seguridad.

El protocolo ICMP está disponible tanto para IPv4 como para IPv6. El protocolo de mensajes para IPv4 es ICMPv4. ICMPv6 proporciona estos mismos servicios para IPv6, pero incluye funcionalidad adicional. En este curso, el término ICMP se utilizará para referirse tanto a ICMPv4 como a ICMPv6.

Existen muchos tipos de mensajes de ICMP y muchos motivos por los cuales se envían estos mensajes. Analizaremos algunos de los mensajes más comunes. Los mensajes ICMP comunes a ICMPv4 y a ICMPv6 incluyen lo siguiente:

- Confirmación de host
- Destino o servicio inaccesible
- Tiempo superado
- Redireccionamiento de ruta

Confirmación de host

Se puede utilizar un mensaje de eco de ICMP para determinar si un host está en funcionamiento. El host local envía una petición de eco de ICMP a un host. Si el host se encuentra disponible, el host de destino responde con una respuesta de eco. En la ilustración, puede establecer que existe una solicitud de eco y la respuesta de eco de ICMP. Este uso de los mensajes de eco de ICMP es la base de la utilidad ping.

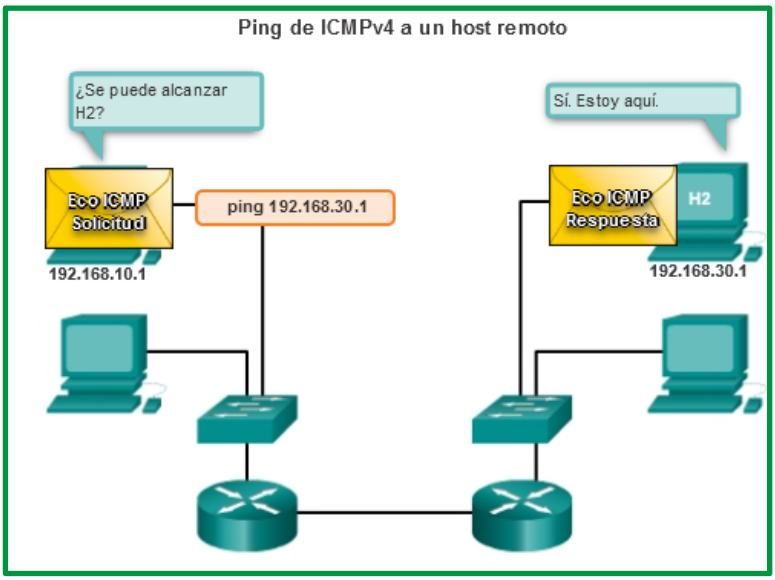


Figure 239. Eco ICMP

Destino o servicio inaccesible

Cuando un host o gateway recibe un paquete que no puede entregar, puede utilizar un mensaje de destino inalcanzable de ICMP para notificar al origen que el destino o el servicio es inalcanzable. El mensaje incluye un código que indica el motivo por el cual no se pudo entregar el paquete.

Algunos de los códigos de destino inalcanzable para ICMPv4 son los siguientes:

- 0: red inalcanzable
- 1: host inalcanzable
- 2: protocolo inalcanzable
- 3: puerto inalcanzable

Los códigos de ICMPv6 para los mensajes de destino inalcanzable son similares, pero presentan algunas diferencias.

Tiempo superado

Los routers utilizan los mensajes de tiempo superado de ICMPv4 para indicar que un paquete no puede reenviarse debido a que el campo Tiempo de vida (TTL) del paquete se disminuyó a 0. Si un router recibe un paquete y disminuye el campo TTL en el paquete IPV4 a cero, descarta el paquete y envía un mensaje de tiempo superado al host de origen.

ICMPv6 también envía un mensaje de tiempo superado si el router no puede reenviar un paquete IPv6 debido a que el paquete caducó. IPv6 no tiene un campo TTL, por lo que utiliza el campo de límite de saltos para determinar si el paquete caducó.

Redireccionamiento de ruta

Un router puede usar un mensaje de redireccionamiento de ICMP para notificar a los hosts de una red acerca de una mejor ruta disponible para un destino en particular. Es posible que este

mensaje sólo pueda usarse cuando el host de origen esté en la misma red física que ambos gateways.

Tanto ICMPv4 como ICMPv6 utilizan mensajes de redireccionamiento de ruta.

Los mensajes informativos y de error que se encuentran en ICMPv6 son muy similares a los mensajes de control y de error que implementa ICMPv4. Sin embargo, ICMPv6 tiene nuevas características y funcionalidad mejorada que no se encuentran en ICMPv4.

ICMPv6 incluye cuatro nuevos protocolos como parte del protocolo ND o NDP (Neighbor Discovery Protocol, protocolo de descubrimiento de vecinos):

- Mensaje de solicitud de router
- Mensaje de anuncio de router
- Mensaje de solicitud de vecino
- Mensaje de anuncio de vecino

Mensajes de solicitud y de anuncio de router

Los dispositivos con IPv6 habilitado pueden dividirse en dos categorías: routers y hosts. Los mensajes de solicitud de router y de anuncio de router se envían entre hosts y routers.

- ***Mensaje de solicitud de router (RS):*** Cuando un host está configurado para obtener la información de direccionamiento de forma automática mediante la configuración automática de dirección sin estado (SLAAC), el host envía un mensaje de RS al router. El mensaje de RS se envía como un mensaje IPv6 multicast de todos los routers.
- ***Mensaje de anuncio de router (RA)***:Los routers envían mensajes de RA para proporcionar información de direccionamiento a los hosts mediante SLAAC. El mensaje de RA puede incluir información de direccionamiento para el host, como el prefijo y la duración de prefijo. Los routers envían mensajes de RA de forma periódica o en respuesta a un mensaje de RS. De manera predeterminada, los routers Cisco envían mensajes de RA cada 200 segundos. Los mensajes de RA se envían a la dirección IPv6 multicast de todos los nodos. Los hosts que utilizan SLAAC establecen su gateway predeterminado en la dirección link-local del router que envió el mensaje de RA.

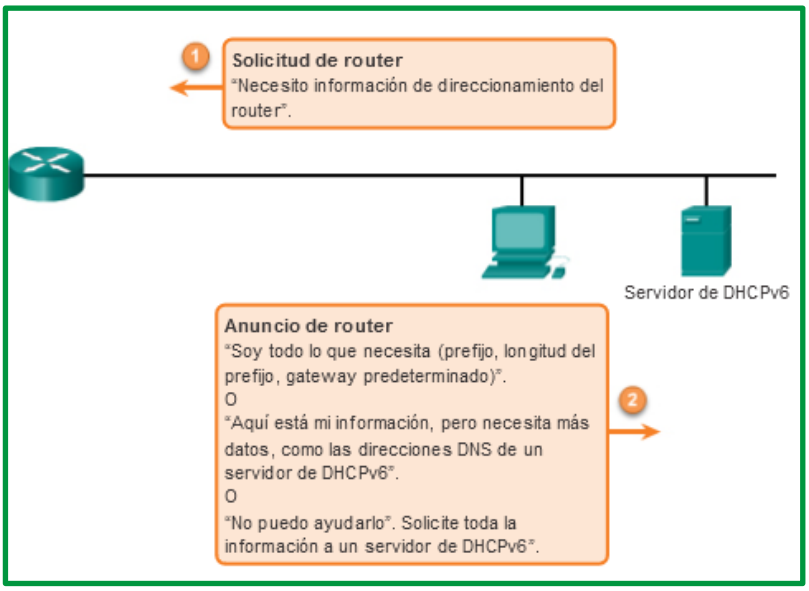


Figure 240. Mensaje de solicitud y anuncio de router

El protocolo de descubrimiento de vecinos de ICMPv6 incluye dos tipos de mensajes adicionales: mensaje de solicitud de vecino (NS) y mensaje de anuncio de vecino (NA).

Los mensajes de solicitud y de anuncio de vecino se utilizan para lo siguiente:

- Resolución de direcciones
- Detección de direcciones duplicadas (DAD)

Resolución de direcciones

La resolución de direcciones se utiliza cuando un dispositivo en la LAN conoce la dirección IPv6 unicast de un destino, pero no conoce la dirección MAC de Ethernet. Para determinar la dirección MAC del destino, el dispositivo envía un mensaje de NS a la dirección de nodo solicitado. El mensaje incluye la dirección IPv6 conocida (objetivo). El dispositivo que tiene la dirección IPv6 objetivo responde con un mensaje de NA que contiene la dirección MAC de Ethernet.

Detección de direcciones duplicadas

Cuando se asigna una dirección unicast global o una dirección unicast link-local a un dispositivo, se recomienda llevar a cabo la detección de direcciones duplicadas (DAD) en la dirección para asegurarse de que sea única. Para revisar si una dirección es única, el dispositivo envía un mensaje de NS con su propia dirección IPv6 como la dirección IPv6 objetivo. Si otro dispositivo en la red tiene esta dirección, responde con un mensaje de NA. Este mensaje de NA notifica al dispositivo emisor que la dirección está en uso. Si no se devuelve un mensaje de NA correspondiente dentro de determinado período, la dirección unicast es única y su uso es aceptable.

La DAD no es obligatoria, pero en RFC 4861 se recomienda que se realice la DAD en direcciones unicast.

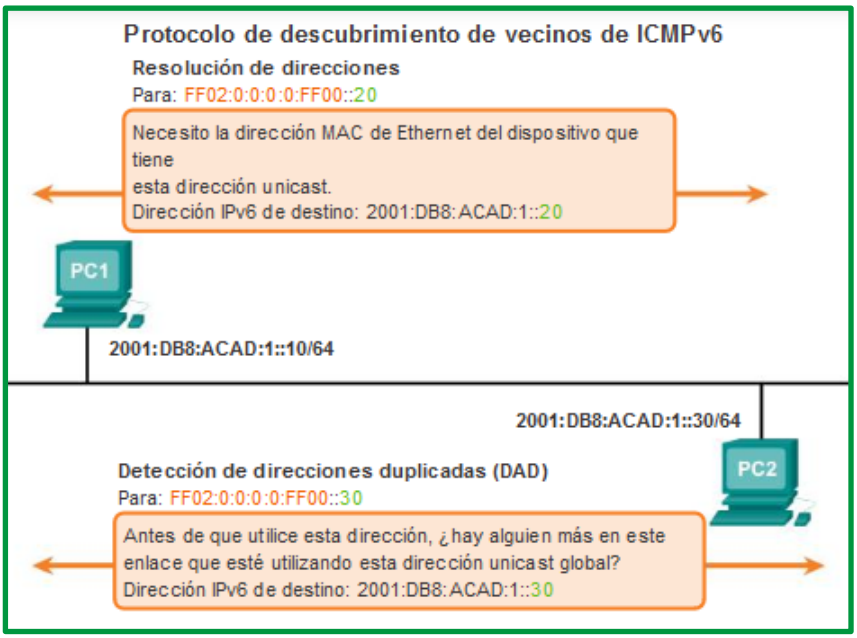


Figure 241. Protocolo de descubrimiento de vecinos de ICMPv6

Enlaces:

RFC 792 http://www.ietf.org/rfc/rfc0792.txt?number=792

RFC 1122 http://www.ietf.org/rfc/rfc1122.txt?number=1122

RFC 2003 http://www.ietf.org/rfc/rfc2003.txt?number=2003

Casos prácticos

Los casos prácticos de la presente unidad se encuentran subida en la siguiente dirección web https://drive.google.com/drive/folders/1aQ7ZVw4OzWNYmUcCX5HAIftf0Lezr7vB?usp=sharing

Bibliografía

Universidad de Salamanca. (27 de 06 de 2011). Recuperado el 20 de 06 de 2021, de http://campus.usal.es/

Área de Ingeniería Telemática. (s.f.). *Universidad Pública de Navarra*. Recuperado el 19 de 06 de 2021, de http://www.tlm.unavarra.es

Calvo, R. A. (s.f.). *Universidad de Cantabria*. Recuperado el 19 de 06 de 2021, de Grupo de Ingeniería Telemática (GIT): https://www.tlmat.unican.es/

ccnadesdecero.com. (s.f.). *CCNA Desde Cero.* Recuperado el 26 de 05 de 2021, de https://ccnadesdecero.com/curso/tipos-de-direcciones-ipv6/

Cisco Networking Academy ITESA. (s.f.). *nstituto Tecnológico Superior del Oriente del Estado de Hidalgo*. Recuperado el 27 de 06 de 2021, de https://www.itesa.edu.mx/netacad/

Class Virtual. (s.f.). Recuperado el 26 de 05 de 2021, de https://eclassvirtual.com/tipos-de-direcciones-ipv6-cisco-ccna/

Deep Medhi, K. R. (s.f.). Recuperado el 19 de 06 de 2021

Fernando Boronat Seguí, M. M. (2013). *Direccionamiento e Interconexión de redes basadas en TCP/IP* (Primera edición, 2013 ed.). Universidad Politécnica de Válencia. Recuperado el 20 de 06 de 2021, de www.editorial.upv.es

Ginno Millán, G. F. (17 de 10 de 2018). A Simple and Fast Algorithm for Traffic Flow . 4. doi:10.1109/ICA-ACCA.2018.8609857

Goitia, M. J. (s.f.). *UNIVERSIDAD NACIONAL DEL NORDESTE*. Recuperado el 19 de 06 de 2021, de http://exa.unne.edu.ar/informatica/SO/ProtocolosRed.PDF

Gutiérrez, A. E. (s.f.). *OpenCourseWare* . Recuperado el 20 de 06 de 2021, de https://ocw.unican.es/pluginfile.php/1357/course/section/1682/Tema%202.pdf

Hernández, M. Á. (09 de 2009). *Universidad de Valladolid*. Recuperado el 12 de 06 de 2021, de Escuela Técnica Su perior de telecomunicación: http://www.tel.uva.es

Leiva, Y. E. (09 de 2014). *http://www.inf.udec.cl*. Recuperado el 12 de 06 de 2021, de http://www.inf.udec.cl

Pedraza, L. F. (11 de 12 de 20211). Enrutamiento basado en el algoritmo de Dijkstra para una red de radio cognitiva. *15*(30). doi:ISSN 0123-921X

Unidersidad de Valencia. (s.f.). *Departamento de Informatica*. Recuperado el 26 de 05 de 2021, de http://informatica.uv.es/iiguia/AER/Tema6_IPX.pdf

Universidad de Oviedo. (05 de 03 de 2012). *Departamento de Ingeniería Eléctrica, Electrónica, de Computadores y de Sistemas*. Recuperado el 12 de 06 de 2021, de http://www.isa.uniovi.es/docencia/redes/

El contenido y gráficos de este compendio han sido obtenido mayoritariamente del curso CCNA de la academia de CISCO, información complementada con información de sitios web que se establecen en las referencias bibliográfica.

Índice

Tabla de contenido

Organización de la lectura para el estudiante por semana del compendio

Semanas	Paginas
Semana 13	Página 3 - 34
Semana 14	Página 34 - 44
Semana 15	Página 44 – 52
Semana 16	Retroalimentación para Examen Final

Resultado de aprendizaje de la asignatura

Conocer los principios básicos, componentes, dispositivos, protocolos, estándares y demás elementos que intervienen en una red de comunicación.

REDES DE COMPUTADORAS

Unidad 4: **Protocolos de Capa de Transporte**

Resultado de aprendizaje de la unidad:

Escoger herramientas de redes para analizar la información que se transmite con cualquier protocolo básico de una arquitectura.

Comprender el proceso aplicado para establecer la conexión de un extremo a otro, analizando los protocolos y técnicas utilizadas que permiten mantener circuitos de comunicación y el control del mismo que garantizan las comunicaciones entre las aplicaciones de los usuarios finales, equipos y dispositivos de red.

Tema 1: Capa de Transporte

La capa de Transporte permite la segmentación de datos y brinda el control necesario para reensamblar las partes dentro de los distintos streams de comunicación.

Las principales responsabilidades de los protocolos de la capa de transporte son las siguientes:

- Rastreo de comunicación individual entre aplicaciones en los hosts de origen y destino.
- División de los datos en segmentos para su administración y reunificación de los datos segmentados en streams de datos de aplicación en el destino.
- Identificación de la aplicación correspondiente para cada stream de comunicación.

Rastreo de conversaciones individuales.

En la capa de transporte, cada conjunto de datos particular que fluye entre una aplicación de origen y una de destino se conoce como “conversación” (figura). Un host puede tener varias aplicaciones que se comunican a través de la red de forma simultánea. Cada una de estas aplicaciones se comunica con una o más aplicaciones en uno o más hosts remotos. Es responsabilidad de la capa de transporte mantener y hacer un seguimiento de todas estas conversaciones.

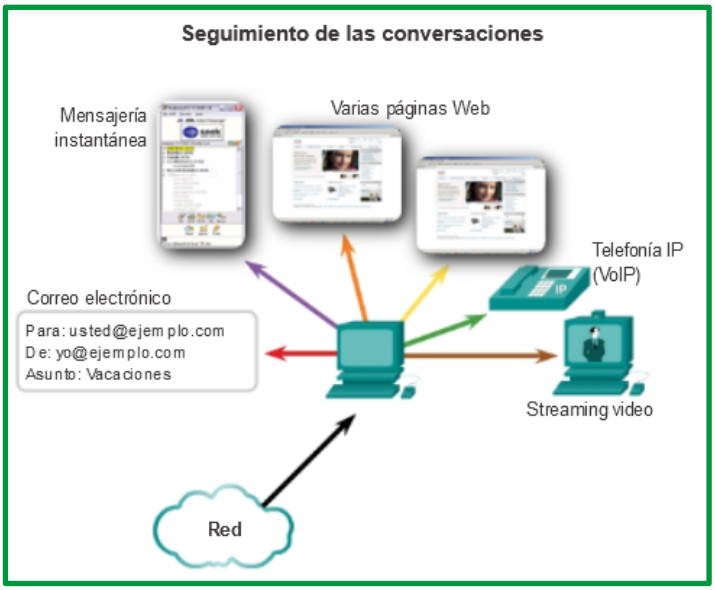


Figure 1. Seguimiento de las comunicaciones

Segmentación de datos y rearmado de segmentos

Se deben preparar los datos para el envío a través de los medios en partes manejables. La mayoría de las redes tienen un límite de la cantidad de datos que se puede incluir en un solo paquete. Los protocolos de la capa de transporte tienen servicios que segmentan los datos de aplicación en bloques de datos de un tamaño apropiado (figura siguiente). Estos servicios incluyen la encapsulación necesaria en cada porción de datos. Se agrega un encabezado a cada bloque de datos para el rearmado. Este encabezado se utiliza para hacer un seguimiento del stream de datos.

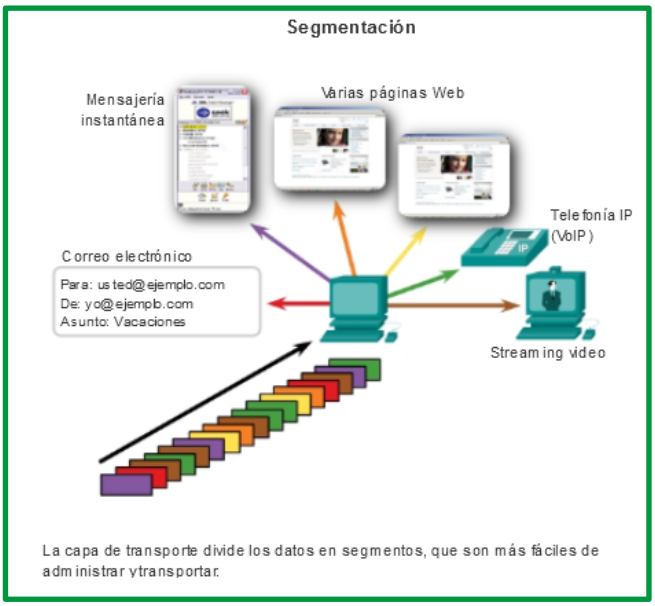


Figure 2. Segmentación de datos

En el destino, la capa de transporte debe poder reconstruir las porciones de datos en un stream de datos completo que sea útil para la capa de aplicación. Los protocolos en la capa de transporte describen cómo se utiliza la información del encabezado de dicha capa para rearmar las porciones de datos en streams para pasarlos a la capa de aplicación.

Identificación de aplicaciones

Puede haber muchas aplicaciones o servicios que se ejecutan en cada host de la red. Para pasar streams de datos a las aplicaciones adecuadas, la capa de transporte debe identificar la aplicación objetivo (figura siguiente). Para lograr esto, la capa de transporte asigna un identificador a cada aplicación. Este identificador se denomina “número de puerto”. A todos los procesos de software que requieran acceder a la red se les asigna un número de puerto exclusivo en ese host. La capa de transporte utiliza puertos para identificar la aplicación o el servicio. +

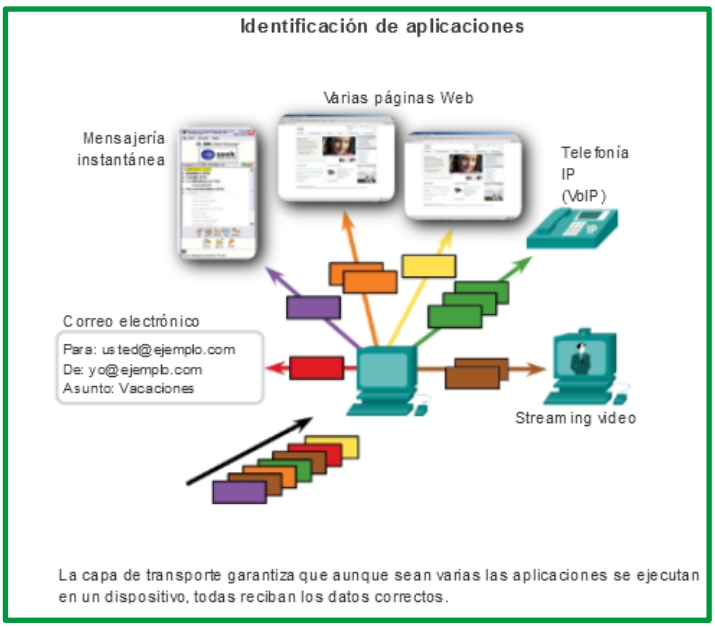


Figure 3.Identificación de aplicaciones.

Las redes de datos e internet brindan soporte a la red humana por medio del suministro de comunicación confiable entre personas. En un único dispositivo, las personas pueden utilizar varias aplicaciones y diversos servicios, como correo electrónico, la Web y la mensajería instantánea, para enviar mensajes o recuperar información. Las aplicaciones, como los clientes de correo electrónico, los exploradores Web y los clientes de mensajería instantánea, permiten que las personas usen PC y redes para enviar mensajes y encontrar información.

Los datos de cada una de estas aplicaciones se empaquetan, se transportan y se entregan a la aplicación correspondiente en el dispositivo de destino. Los procesos que se describen en la capa de transporte del modelo OSI aceptan los datos de la capa de aplicación y los preparan para el direccionamiento en la capa de red. La capa de transporte prepara los datos para transmitirlos a través de la red. La PC de origen se comunica con una PC receptora para decidir cómo dividir los datos en segmentos, cómo asegurarse de que ninguno de los segmentos se pierda y cómo verificar si llegan todos los segmentos. Al considerar la capa de transporte, imagínese un departamento de envíos que prepara un único pedido de varios paquetes para entregar.

La capa de transporte no tiene conocimiento del tipo de host de destino, el tipo de medio por el que deben viajar los datos, la ruta tomada por los datos, la congestión en un enlace o el tamaño de la red.

La capa de transporte incluye los protocolos:

- Protocolo de Control de Transmisión: **Transmission Control Protocol (TCP)**
- Protocolo de Datagramas de Usuario: **User Datagram Protocol (UDP)**
- Protocolo de transmisión de control de flujo: **Stream Control Transmission Protocol (SCTP)**


Recuerde que. – La capa de transporte mueve datos entre aplicaciones en dispositivos en la red.

En esta unidad, se examina el rol de la capa de transporte en las redes de comunicaciones. La capa de transporte incluye también las siguientes funciones:

- Permite que varias aplicaciones, como el envío de correo electrónico y las redes sociales, se puedan comunicar a través la red al mismo tiempo en un único dispositivo.
- Asegura que, si es necesario, la aplicación correcta reciba todos los datos con confianza y en orden.
- Emplea mecanismos de manejo de errores.

Objetivos de aprendizaje

Al completar la presente unidad, usted podrá:

- Explicar la necesidad de la capa de transporte.

- Identificar la función de la capa de transporte a medida que provee la transferencia de datos de extremo a extremo entre las aplicaciones.
- Describir la función de dos protocolos de la capa de transporte TCP/IP: TCP y UDP.
- Explicar las funciones clave de la capa de transporte, incluso la confiabilidad, el direccionamiento de puerto y la segmentación.
- Explicar cómo cada TCP y UDP maneja las funciones clave.
- Identificar cuándo es apropiado usar TCP o UDP y proveer ejemplos de aplicaciones que usan cada protocolo.

IP solo se refiere a la estructura, direccionamiento y enrutamiento de paquetes. IP no especifica cómo se realiza la entrega o el transporte de los paquetes.

Protocolos de Capa de Transporte

Los protocolos de la capa de transporte especifican cómo transferir mensajes entre hosts y son responsables de administrar los requisitos de confiabilidad de una conversación. La capa de transporte incluye los protocolos TCP, UDP y SCTP.

Las diferentes aplicaciones tienen diferentes requisitos de fiabilidad de transporte. Por lo tanto, TCP/IP proporciona dos protocolos de capa de transporte.

Servicio de transporte

La capa de transporte es responsable de establecer una sesión de comunicación temporal entre dos aplicaciones y de transmitir datos entre ellas. Las aplicaciones generan los datos que se envían de una aplicación en un host de origen a una aplicación a un host de destino, independientemente del tipo de host de destino, el tipo de medios a través de los que deben viajar los datos, la ruta que toman los datos, la congestión en un enlace o el tamaño de la red. Como se muestra en la ilustración, la capa de transporte es el enlace entre la capa de aplicación y las capas inferiores que son responsables de la transmisión a través de la red.

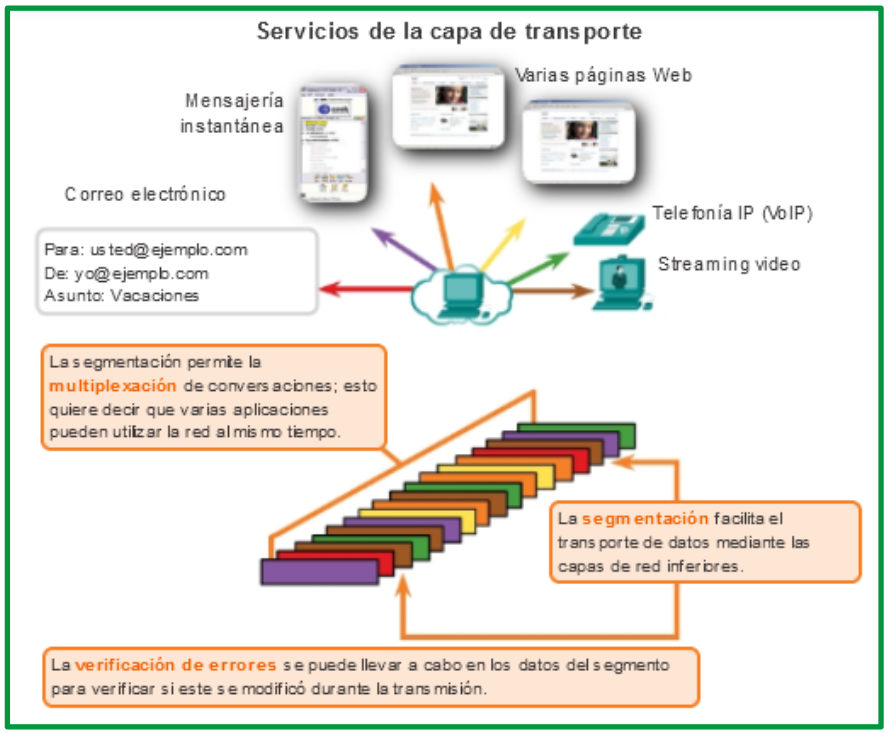


Figure 4. Servicios de la capa de transporte

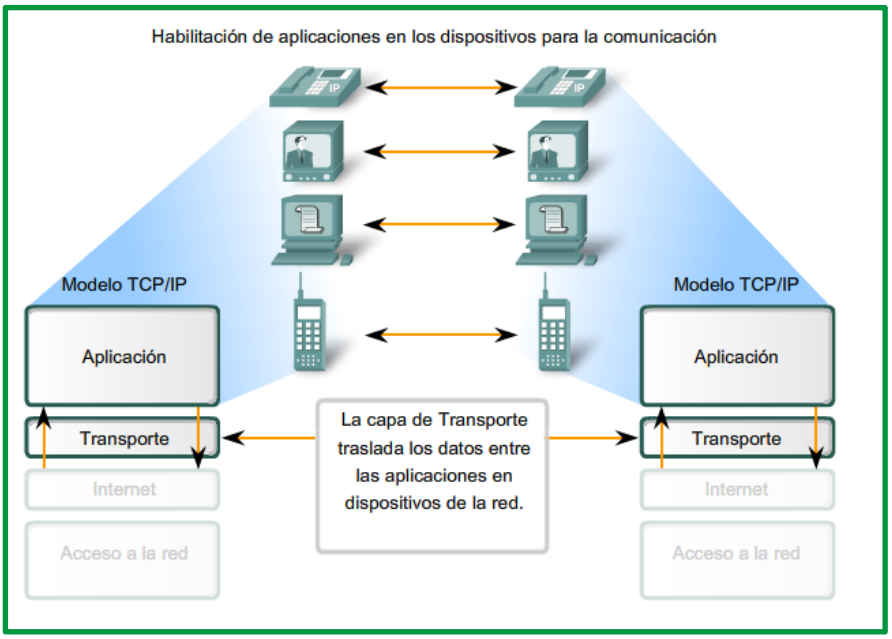


Figure 5. Capa de Transporte traslada los datos en el dispositivo de la red

La capa de transporte proporciona un método para entregar datos a través de la red de una manera que garantiza que estos se puedan volver a unir correctamente en el extremo receptor. La capa de transporte permite la segmentación de datos y proporciona el control necesario para rearmar estos segmentos en los distintos streams de comunicación. En el protocolo TCP/IP, estos procesos de segmentación y rearmado se pueden lograr utilizando dos protocolos muy diferentes de la capa de transporte: el protocolo de control de transmisión (TCP) y el protocolo de datagramas de usuario (UDP).

Los servicios que ofrece la capa de transporte están orientados a la conexión por medio de protocolos como el TPC y SCTP; mientras que los protocolos UPD ofrecen un servicio no orientado a la conexión.

Los servicios que un protocolo de transporte puede ofrecer están condicionados por el modelo de servicio del protocolo de la capa de red subyacente. Si la capa de red no garantiza un retardo máximo o un ancho de banda mínimo para las T-PDUs, la capa de transporte tampoco lo puede garantizar a la capa de aplicación; sin embargo, la capa de transporte puede ofrecer ciertos servicios, aunque la capa de red no.

El servicio orientado a conexión es un servicio seguro extremo a extremo que se utiliza sobre redes inseguras que pueden perder, dañar, almacenar o duplicar paquetes donde se establecen tres pasos básicos: establecimiento, transferencia de datos, y liberación; mientras que en el servicio no orientado a la conexión se tratan los paquetes de forma individual.

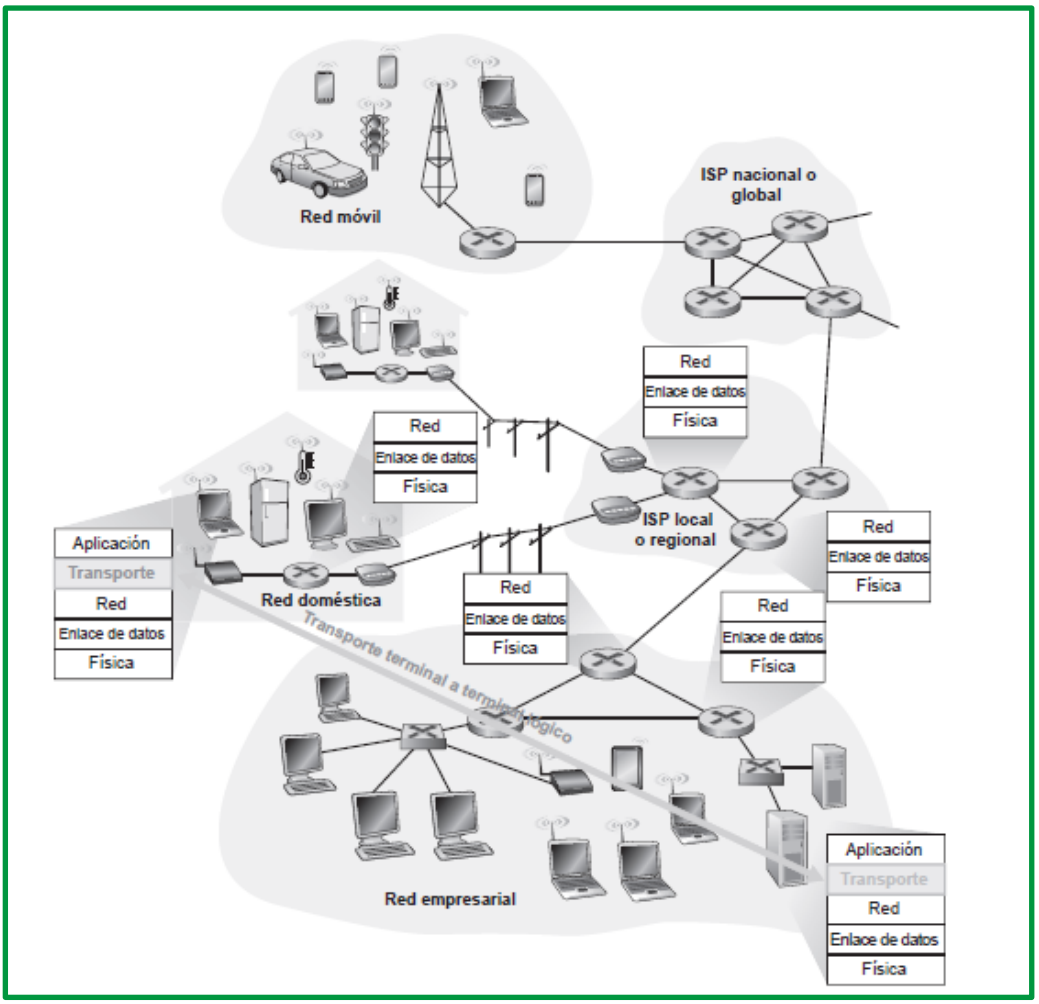


Figure 6. La capa de transporte proporciona una comunicación lógica
Fuente: Libro Redes de computadoras. Un enfoque descendente, 7 Edición.

En la gráfica se puede determinar lo siguiente:

- Las aplicaciones usan esta comunicación lógica que proporciona la capa de transporte para enviar los mensajes libres de preocupaciones de la capa física.

- El emisor fragmenta los mensajes de aplicación en segmentos y los pasa a la capa de red.
- El receptor reagrupa los segmentos en mensajes y los pasa a la capa de aplicación.

Elementos de los protocolos de transporte

Para cumplir correctamente las funciones, los protocolos de la capa de transporte se componen de elementos para mantener una comunicación confiable, se detallan los elementos que utilizan los protocolos de transporte:

- Transferencia confiable de datos
- Direccionamiento
- Establecimiento de una conexión
- Liberalización de una conexión
- Control de flujo
- Multiplexación y demultiplexación

Transferencia confiable de datos

Un protocolo de transporte fiable de datos significa **IMPLEMENTAR** esta abstracción del servicio.

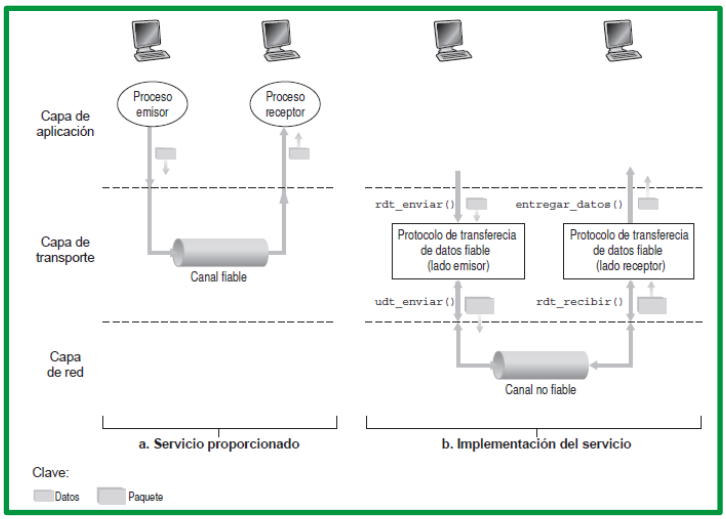


Figure 7. Transferencia de datos fiable: modelo del servicio e implementación del servicio
Fuente: Libro Redes de computadoras. Un enfoque descendente, 7 Edición

Se puede determinar que se consideran los siguientes aspectos:

- ***Transferencia de datos fiable sobre un canal totalmente fiable***. En primer lugar, consideremos el caso más simple, en el que el canal subyacente es completamente fiable.
- ***Transferencia fiable de datos sobre un canal con errores de bits***. Un modelo más realista del canal subyacente sería uno en el que los bits de un paquete pudieran corromperse. Tales errores de bit se producen en los componentes físicos de una red cuando un paquete se transmite, se propaga o accede a un buffer.

  En un escenario típico, la persona que escucha el mensaje podría decir "***De acuerdo***" después de cada frase que escuche, comprenda y apunte. Si la persona que escucha el mensaje no oye una frase, le pedirá que la ***repita***. Este protocolo de dictado de mensajes utiliza tanto ***reconocimientos positivos*** ("***De acuerdo***") como ***reconocimientos negativos***

("***Por favor, repita***"). Estos mensajes de control permiten al receptor hacer saber al emisor qué es lo que ha recibido correctamente y qué ha recibido con errores y por tanto debe repetir. En una red de computadoras, los protocolos de transferencia de datos fiables basados en tales retransmisiones se conocen como ***protocolos ARQ*** (Automatic Repeat reQuest, Solicitud automática de repetición).

En los protocolos ARQ se requieren, fundamentalmente, tres capacidades de protocolo adicionales para gestionar la presencia de errores de bit:

- ***Detección de errores***. En primer lugar, se necesita un mecanismo que permita al receptor detectar que se han producido errores de bit. Recuerde de la sección anterior que UDP utiliza el campo de suma de comprobación de Internet precisamente para este propósito
- ***Realimentación del receptor***. Dado que el emisor y el receptor normalmente se ejecutan en sistemas terminales diferentes, posiblemente separados por miles de kilómetros, la única forma de que el emisor sepa lo que ocurre en el receptor (en este caso, si un paquete ha sido recibido correctamente o no) es que el receptor envíe explícitamente información de realimentación al emisor. Las respuestas de acuse de recibo o ***reconocimiento positivo*** (**ACK**) y ***reconocimiento negativo*** (**NAK**).
- ***Retransmisión***. Un paquete que se recibe con errores en el receptor será retransmitido por el emisor.

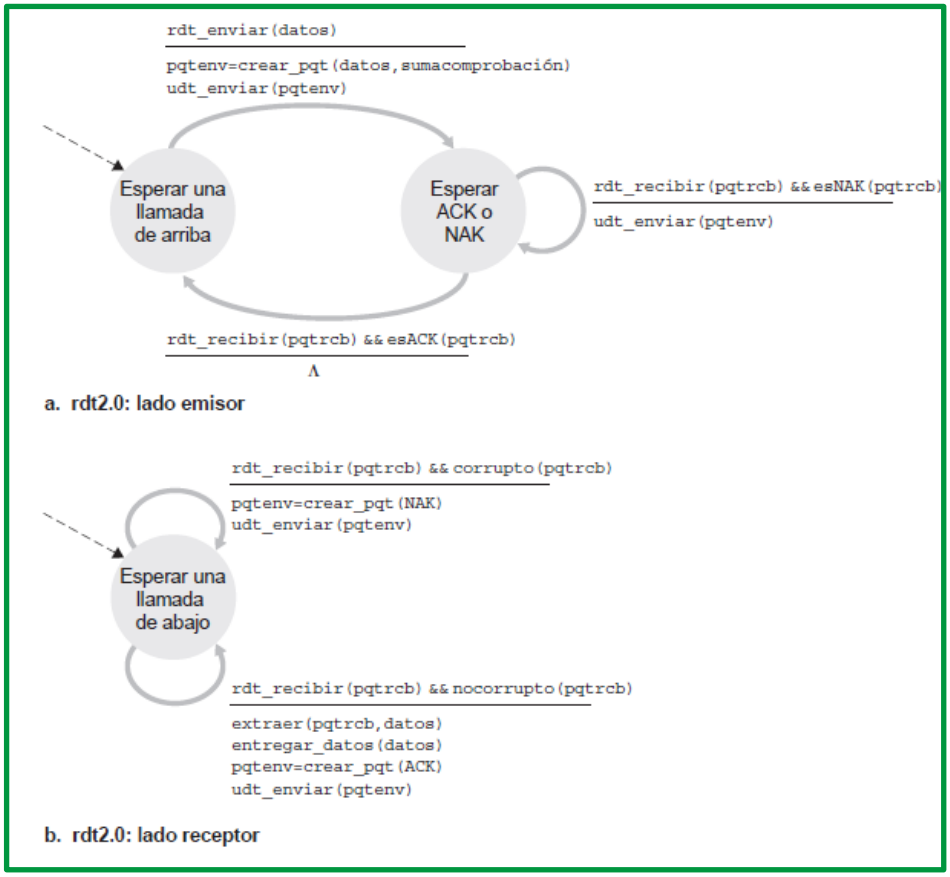


Figure 8. Protocolo para un canal con errores de bit.
Fuente: Libro Redes de computadoras. Un enfoque descendente, 7 Edición

- ***Transferencia fiable de datos sobre un canal con pérdidas y errores de bits***. Suponga ahora que además de bits corrompidos, el canal subyacente también puede perder paquetes, un suceso no desconocido en las redes de computadoras de hoy en día (incluyendo Internet). Por tanto, ahora el protocolo tiene que preocuparse por dos problemas más: cómo detectar la pérdida de paquetes y qué hacer cuando se pierde un paquete. El uso de la suma de comprobación (***cheksum***), los ***números de secuencia***, los ***paquetes ACK*** y la ***retransmisión de paquetes***, técnicas desarrolladas van a permitir abordar este último problema.

  La solución es aplicar mecanismos, se recomienda revisar la lectura complementaria para entender el funcionamiento de estas técnicas, se detallan las siguientes:

  - Protocolo de bit alternante
  - Protocolo de parada y espera
  - Protocolo con procesamiento en cadena
  - Protocolo GBN (Go-Back-N, Retroceder N)
  - Repetición selectiva (SR).

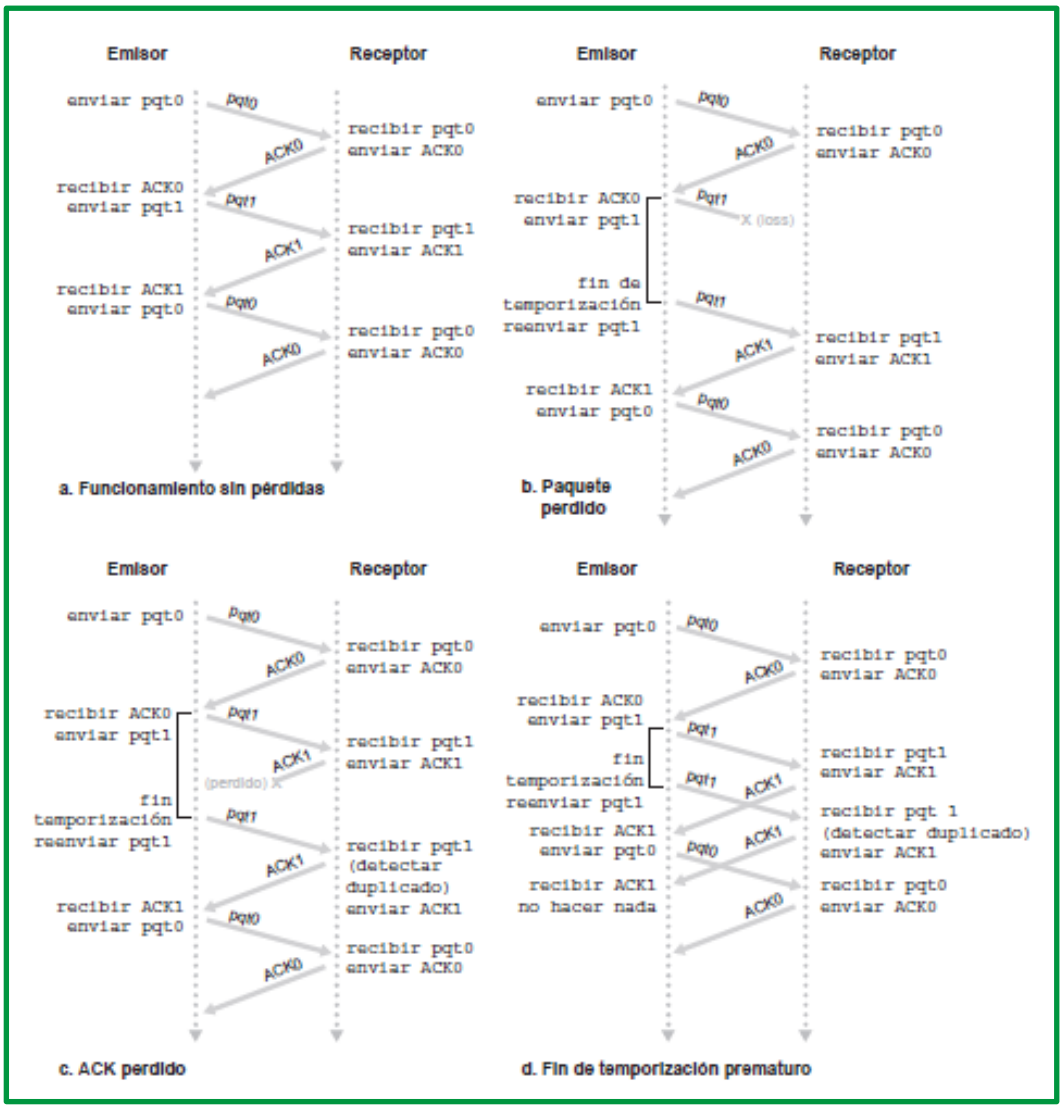


Figure 9. Protocolo de bit alternante

Fuente: Libro Redes de computadoras. Un enfoque descendente, 7 Edición

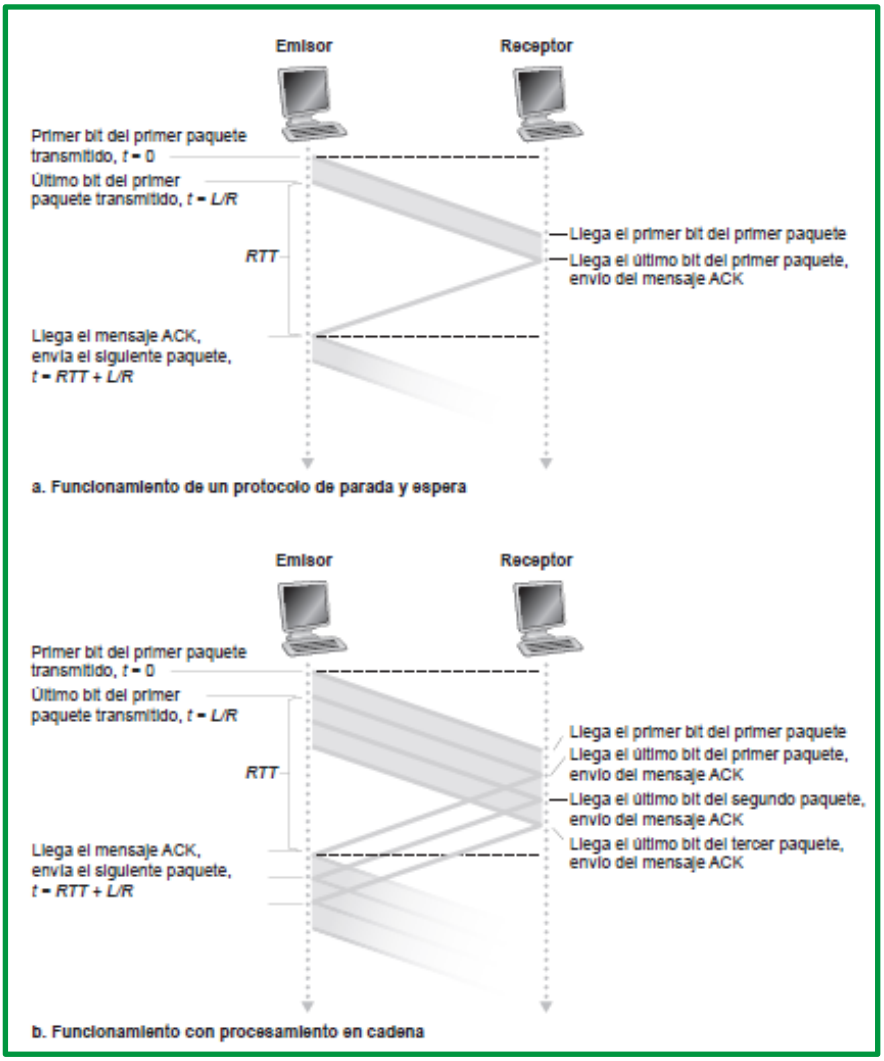


Figure 10.Proceso de transmisión con un protocolo de parada y espera y un protocolo con procesamiento en cadena
Fuente: Libro Redes de computadoras. Un enfoque descendente, 7 Edición

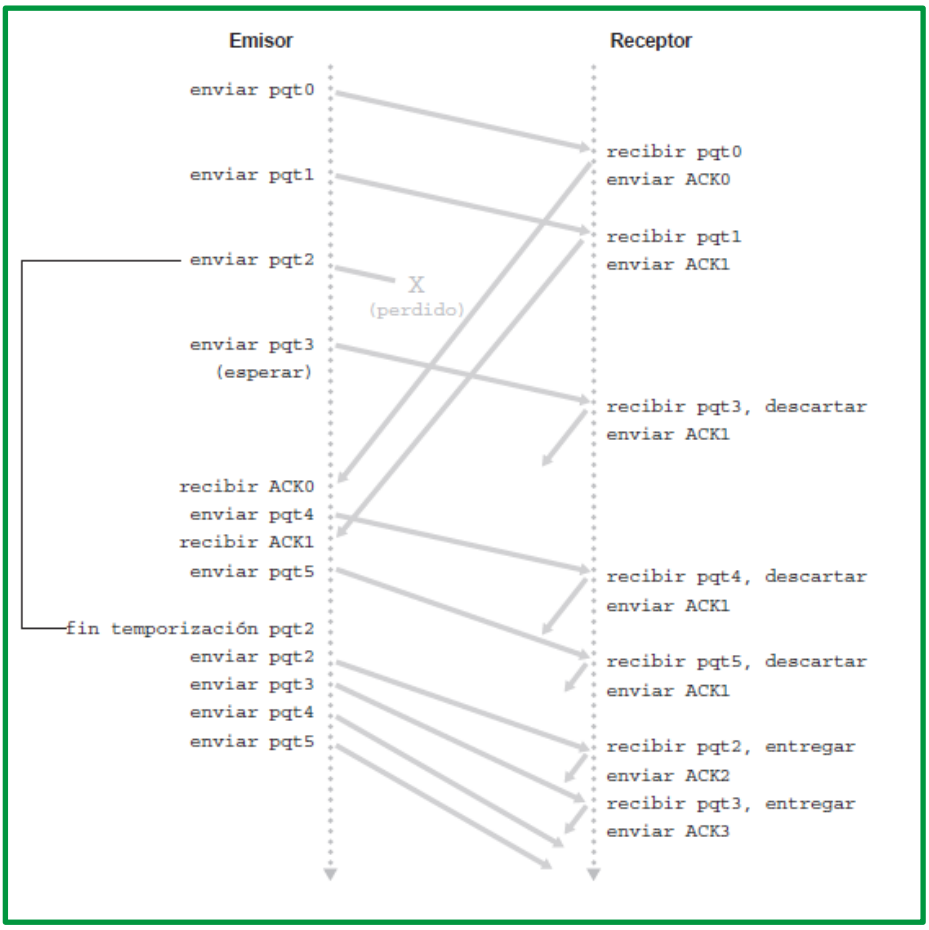


Figure 11. Funcionamiento del protocolo GBN (retroceder N)
Fuente: Libro Redes de computadoras. Un enfoque descendente, 7 Edición

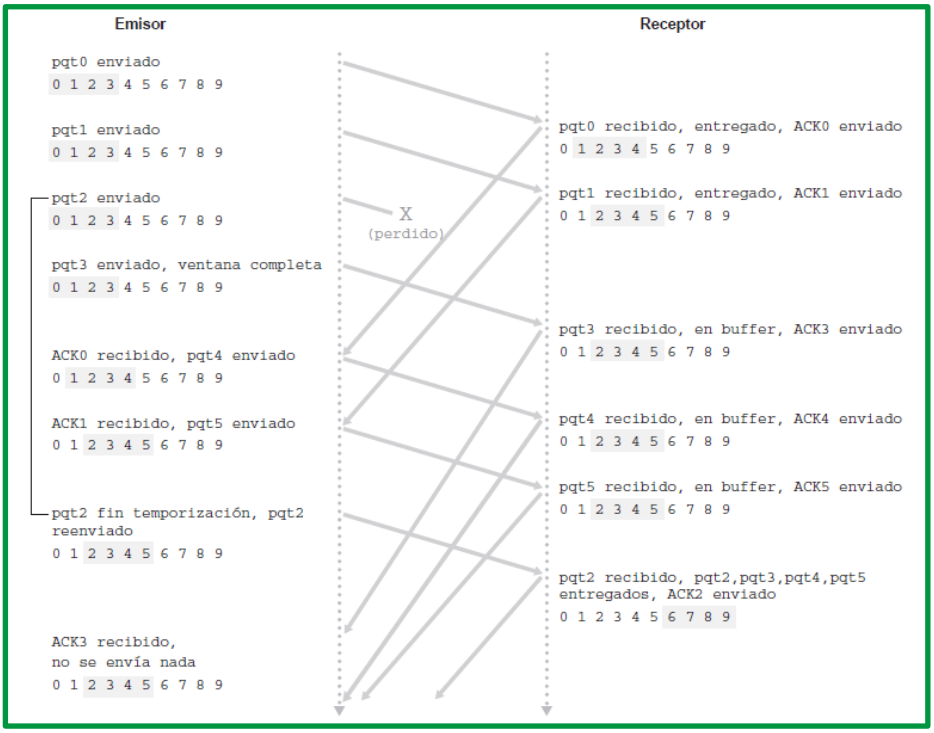


Figure 12. Funcionamiento del protocolo SR.
Fuente: Libro Redes de computadoras. Un enfoque descendente, 7 Edición

Podemos establecer la tabla publicada en el libro de Redes de computadoras: un enfoque descendente de la séptima edición en el cual resumen de los mecanismos para la transferencia de datos fiable y su uso.

Mecanismo	Uso, Comentarios
Suma de comprobación (Checksum)	Utilizada para detectar errores de bit en un paquete transmitido.
Temporizador	Se emplea para detectar el fin de temporización y retransmitir un paquete, posiblemente porque el paquete (o su mensaje ACK correspondiente) se ha perdido en el canal. Puesto que se puede producir un fin de temporización si un paquete está retardado pero no perdido (fin de temporización prematura), o si el receptor ha recibido un paquete pero se ha perdido el correspondiente ACK del receptor al emisor, puede ocurrir que el receptor reciba copias duplicadas de un paquete.
Número de secuencia	Se emplea para numerar secuencialmente los paquetes de datos que fluyen del emisor hacia el receptor. Los saltos en los números de secuencia de los paquetes recibidos permiten al receptor detectar que se ha perdido un paquete. Los paquetes con números de secuencia duplicados permiten al receptor detectar copias duplicadas de un paquete.
Reconocimiento (ACK)	El receptor utiliza estos paquetes para indicar al emisor que un paquete o un conjunto de paquetes ha sido recibido correctamente. Los mensajes de reconocimiento suelen contener el número de secuencia del paquete o los paquetes que están confirmando. Dependiendo del protocolo, los mensajes de reconocimiento pueden ser individuales o acumulativos.
Reconocimiento negativo (NAK)	El receptor utiliza estos paquetes para indicar al emisor que un paquete no ha sido recibido (NAK) correctamente. Normalmente, los mensajes de reconocimiento negativo contienen el número de secuencia de dicho paquete erróneo.
Ventana, procesamiento en cadena	El emisor puede estar restringido para enviar únicamente paquetes cuyo número de secuencia caiga dentro de un rango determinado. Permitiendo que se transmitan varios paquetes aunque no estén todavía reconocidos, se puede incrementar la tasa de utilización del emisor respecto al modo de operación de los protocolos de parada y espera. Veremos brevemente que el tamaño de la ventana se puede establecer basándose en la capacidad del receptor para recibir y almacenar en buffer los mensajes, o en el nivel de congestión de la red, o en ambos parámetros.

Figure 13. resumen de los mecanismos para la transferencia de datos fiable y su uso
Fuente: Libro Redes de computadoras. Un enfoque descendente, 7 Edición

Direccionamiento

En algunas definiciones en la web se determina que cuando un proceso desea establecer una conexión con un computador de aplicación remoto, debe especificar a cuál se conectará (¿a quién le llegará el mensaje?). El método que normalmente se emplea es definir direcciones de transporte en las que los procesos pueden estar a la escucha de solicitudes de conexiones. En Internet, estos puntos terminales se denominan puertos, pero usaremos el término genérico de TSAP (Punto de Acceso al Servicio de Transporte). Los puntos terminales análogos de la capa de red se llaman NSAP (Punto de Acceso al Servicio de Red). Las direcciones IP son ejemplos de NSAPs.

En el encabezado de cada segmento o datagrama, hay un puerto origen y uno de destino. El número de ***puerto de origen*** es el número para esta comunicación asociado con la aplicación que origina la comunicación en el host local. Como se muestra en la ilustración, el número de puerto de destino es el número para esta comunicación relacionada con la aplicación de destino en el host remoto.

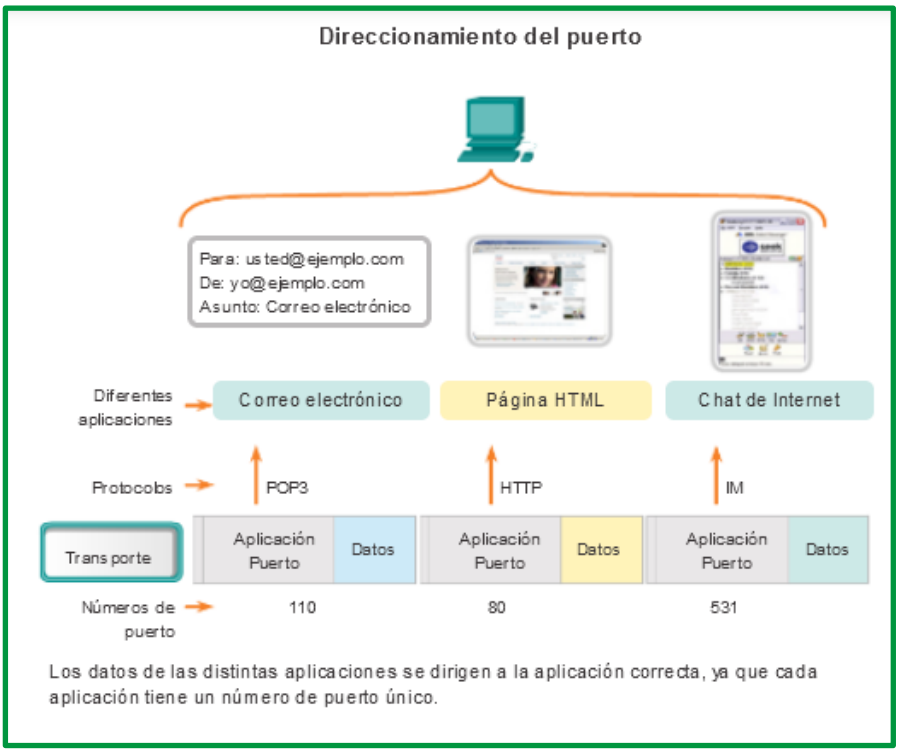


Figure 14. Puertos

Cuando se envía un mensaje utilizando TCP o UDP, los protocolos y servicios solicitados se identifican con un número de puerto. ***Un puerto*** es un identificador numérico de cada segmento, que se utiliza para realizar un seguimiento de conversaciones específicas y de servicios de destino solicitados. Cada mensaje que envía un host contiene un puerto de origen y un puerto de destino.

Puerto de destino

El cliente coloca un número de puerto de destino en el segmento para informar al servidor de destino el servicio solicitado. Por ejemplo: el puerto 80 se refiere a HTTP o al servicio Web. Cuando un cliente especifica el puerto 80 en el puerto de destino, el servidor que recibe el mensaje sabe que se solicitan servicios Web. Un servidor puede ofrecer más de un servicio simultáneamente. Por ejemplo, puede ofrecer servicios Web en el puerto 80 al mismo tiempo que ofrece el establecimiento de una conexión FTP en el puerto 21.

Puerto de origen

El número de puerto de origen es generado de manera aleatoria por el dispositivo emisor para identificar una conversación entre dos dispositivos. Esto permite establecer varias conversaciones simultáneamente. En otras palabras, un dispositivo puede enviar varias solicitudes de servicio HTTP a un servidor Web al mismo tiempo. El seguimiento de las conversaciones por separado se basa en los puertos de origen.

Los puertos de origen y de destino se colocan dentro del segmento. Los segmentos se encapsulan dentro de un paquete IP. El paquete IP contiene la dirección IP de origen y de destino. La combinación de las direcciones IP de origen y de destino y de los números de puerto de origen y de destino se conoce como "***socket***". El ***socket*** se utiliza para identificar el servidor y

el servicio que solicita el cliente. Miles de hosts se comunican a diario con millones de servidores diferentes. Los sockets identifican esas comunicaciones.

La combinación del número de puerto de la capa de transporte y de la dirección IP de la capa de red del host identifica de manera exclusiva un proceso de aplicación en particular que se ejecuta en un dispositivo host individual. Esta combinación se denomina **socket**. Un par de sockets, que consiste en las direcciones IP de origen y destino y los números de puertos, también es exclusivo e identifica la conversación específica entre los dos hosts.

Un socket de cliente puede ser parecido a esto, donde 1099 representa el número de puerto de origen: 192.168.1.5:1099

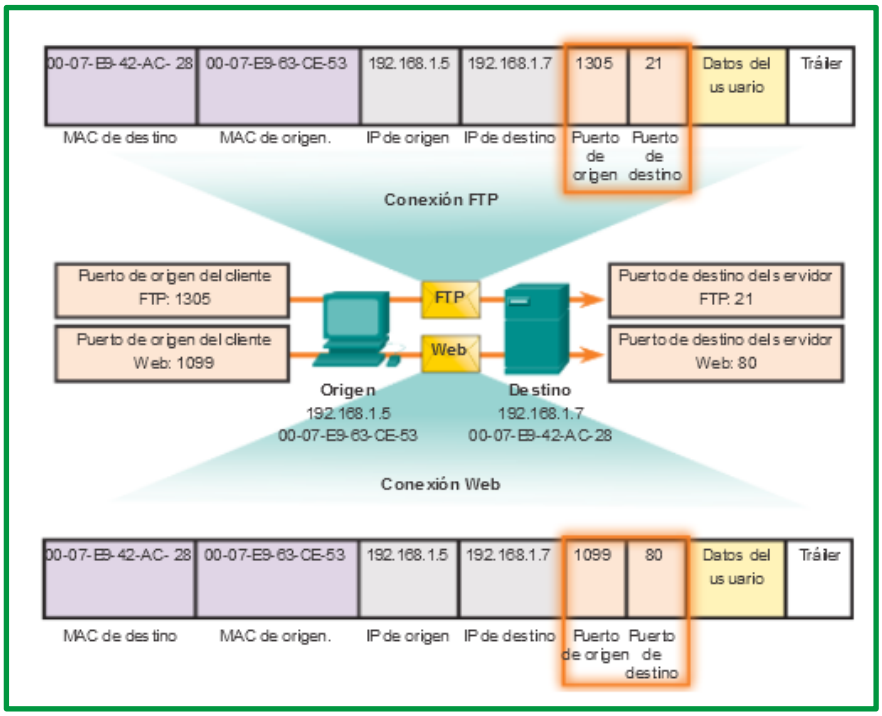


Figure 15. Socket

El socket en un servidor Web podría ser el siguiente: 192.168.1.7:80

Juntos, estos dos sockets se combinan para formar un par de sockets: 192.168.1.5:1099, 192.168.1.7:80

Con la creación de sockets, se conocen los extremos de la comunicación, de modo que los datos puedan moverse desde una aplicación en un host hacia una aplicación en otro host. Los sockets permiten que los procesos múltiples que se ejecutan en un cliente se distingan entre sí. También permiten la diferenciación de múltiples conexiones a un proceso de servidor.

El puerto de origen de la solicitud de un cliente se genera de manera aleatoria. El número de puerto actúa como dirección de retorno para la aplicación que realiza la solicitud. La capa de transporte hace un seguimiento de este puerto y de la aplicación que generó la solicitud de manera que cuando se devuelva una respuesta, esta se envíe a la aplicación correcta. El número de puerto de la aplicación que realiza la solicitud se utiliza como número de puerto de destino en la respuesta que vuelve del servidor.

La Agencia de asignación de números por Internet (IANA) asigna números de puerto. IANA es un organismo normativo responsable de asegurar diferentes estándares de direccionamiento.

Existen diferentes tipos de números de puerto:

- ***Puertos bien conocidos*** (números del 0 al 1023): estos números se reservan para servicios y aplicaciones. Se utilizan comúnmente para aplicaciones como HTTP (servidor Web), protocolo de acceso a mensajes de Internet (IMAP) o protocolo simple de transferencia de correo (SMTP) (servidor de correo electrónico) y Telnet. Al definir estos puertos bien conocidos para las aplicaciones de los servidores, las aplicaciones cliente se pueden programar para solicitar una conexión a ese puerto en particular y el servicio relacionado.
- ***Puertos registrados*** (números del 1024 al 49151): estos números de puerto se asignan a procesos o aplicaciones del usuario. Principalmente, estos procesos son aplicaciones individuales que el usuario elige instalar en lugar de aplicaciones comunes que recibiría un número de puerto bien conocido. Cuando no se utilizan para un recurso del servidor, un cliente puede seleccionar estos puertos de forma dinámica como su puerto de origen.
- ***Puertos dinámicos o privados*** (números 49152 a 65535): también conocidos como puertos efímeros, generalmente se los asigna de forma dinámica a las aplicaciones cliente cuando el cliente inicia una conexión a un servicio. El puerto dinámico suele utilizarse para identificar la aplicación cliente durante la comunicación, mientras que el cliente utiliza el puerto bien conocido para identificar el servicio que se solicita en el servidor y conectarse a dicho servicio. No es común que un cliente se conecte a un servicio mediante un puerto dinámico o privado (aunque algunos programas de intercambio de archivos punto a punto lo hacen).

Figure 16. Puertos bien conocidos y registrados comunes en TCP y UDP.

Uso de TCP y UDP

Algunas aplicaciones pueden utilizar tanto TCP como UDP. Por ejemplo, el bajo gasto de UDP permite que DNS atienda rápidamente varias solicitudes de clientes. Sin embargo, a veces el envío de la información solicitada puede requerir la confiabilidad de TCP. En este caso, el número de puerto bien conocido (53) lo utilizan ambos protocolos con este servicio.

Hay una lista de números de puerto y de aplicaciones asociadas en el sitio Web organizacional de la IANA.

A veces es necesario conocer las conexiones TCP activas que están abiertas y en ejecución en el host de red. ***Netstat*** es una utilidad de red importante que puede usarse para verificar esas conexiones. ***Netstat*** indica el protocolo que se está usando, la dirección y el número de puerto locales, la dirección y el número de puerto externos y el estado de la conexión.

Las conexiones TCP desconocidas pueden presentar una amenaza de seguridad grave, ya que pueden indicar que hay algo o alguien conectado al host local. Además, las conexiones TCP innecesarias pueden consumir recursos valiosos del sistema y, por lo tanto, enlentecer el rendimiento del host. ***Netstat*** debe utilizarse para examinar las conexiones abiertas de un host cuando el rendimiento parece estar comprometido.

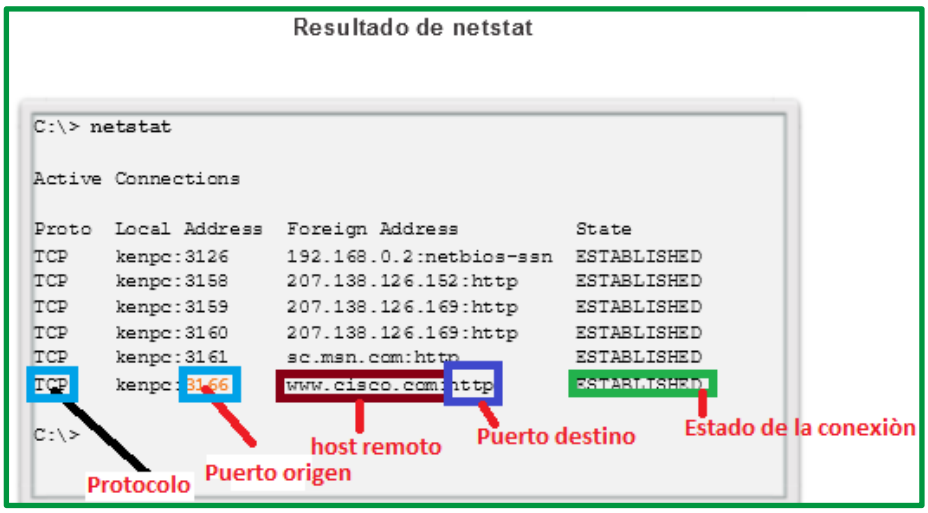


Figure 17. Resultado de comando netstat

En las unidades anteriores, se explicó la forma en que se construyen las unidades de datos del protocolo (PDU) mediante la transmisión de datos de una aplicación a través de los diversos protocolos para crear una PDU que después se transmita en el medio. En el host de destino, este proceso se revierte hasta que los datos se puedan transferir a la aplicación.

Algunas aplicaciones transmiten grandes cantidades de datos; en algunos casos, muchos gigabytes. Resultaría poco práctico enviar todos estos datos en una sola gran sección. No puede transmitirse ningún otro tráfico de red mientras se envían estos datos. Una gran sección de datos puede tardar minutos y hasta horas en enviarse. Además, si hubiese errores, se perdería el archivo de datos completo o habría que volver a enviarlo. Los dispositivos de red no cuentan con buffers de memoria lo suficientemente grandes como para almacenar esa cantidad de datos durante la transmisión o recepción. El límite varía según la tecnología de red y el medio físico específico en uso.

La división de datos de aplicación en segmentos asegura que estos se transmitan dentro de los límites de los medios y que los datos de diferentes aplicaciones se puedan multiplexar en los medios.

TCP y UDP: manejo distinto de la segmentación

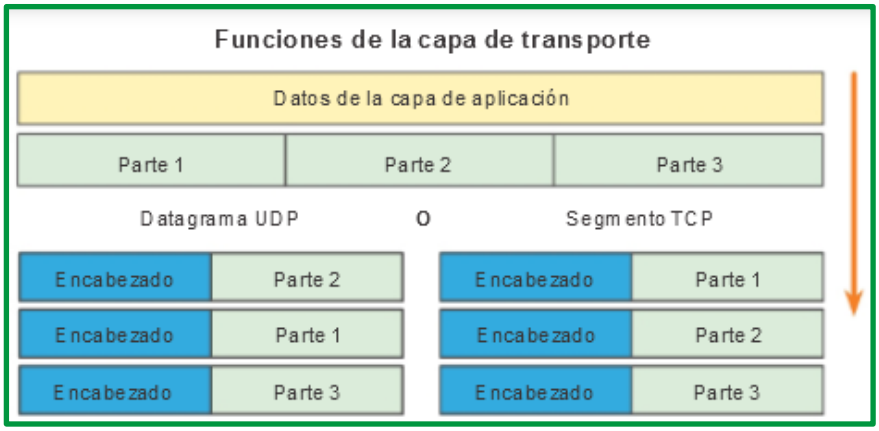


Figure 18. Segmentación de datos

Como se muestra en la ilustración, cada encabezado del segmento TCP contiene un número de secuencia que permite que las funciones de la capa de transporte en el host de destino vuelvan a armar segmentos en el orden en que se transmitieron. Esto asegura que la aplicación de destino tiene los datos en la misma forma que el emisor la planeó.

Aunque los servicios que utilizan UDP rastrean también las conversaciones entre las aplicaciones, no se encargan del orden en que se transmite la información ni de mantener una conexión. No existe número de secuencia en el encabezado UDP. UDP es un diseño simple y genera menos carga que TCP, lo que produce una transferencia de datos más rápida.

La información puede llegar en un orden distinto del de la transmisión, ya que los distintos paquetes pueden tomar diferentes rutas a través de la red. Una aplicación que utiliza UDP debe tolerar el hecho de que los datos no lleguen en el orden en el que fueron enviados.

Establecimiento de una conexión

Para entender con propiedad las diferencias entre TCP y UDP, es importante comprender la manera en que cada protocolo implementa las funciones específicas de confiabilidad y la forma en que realizan el seguimiento de las comunicaciones.

Parte de la carga adicional que genera el uso de TCP es el tráfico de red generado por los acuses de recibo y las retransmisiones. El establecimiento de las sesiones genera sobrecarga en forma de segmentos adicionales que se intercambian. Hay también sobrecarga en los hosts individuales creada por la necesidad de mantener un registro de los segmentos que esperan un acuse de recibo y por el proceso de retransmisión.

Los procesos de las aplicaciones se ejecutan en los servidores. Un único servidor puede ejecutar varios procesos de aplicaciones al mismo tiempo. Estos procesos esperan hasta que el cliente inicia comunicación con una solicitud de información u otros servicios.

Cada proceso de aplicación que se ejecuta en el servidor se configura para utilizar un número de puerto, ya sea predeterminado o de forma manual por el administrador del sistema. Un servidor individual no puede tener dos servicios asignados al mismo número de puerto dentro de los mismos servicios de la capa de transporte. Un host que ejecuta una aplicación de servidor Web y

una de transferencia de archivos no puede configurar ambas para utilizar el mismo puerto (por ejemplo, el puerto TCP 8080). Una aplicación de servidor activa asignada a un puerto específico se considera abierta, lo que significa que la capa de transporte acepta y procesa los segmentos dirigidos a ese puerto. Toda solicitud entrante de una cliente direccionada al socket correcto es aceptada y los datos se envían a la aplicación del servidor. Pueden existir varios puertos simultáneos abiertos en un servidor, uno para cada aplicación de servidor activa. Es común que un servidor proporcione más de un servicio al mismo tiempo, como un servidor Web y un servidor FTP.

Una manera de mejorar la seguridad en un servidor es restringir el acceso al servidor únicamente a aquellos puertos relacionados con los servicios y las aplicaciones a los que deben poder acceder los solicitantes autorizados.

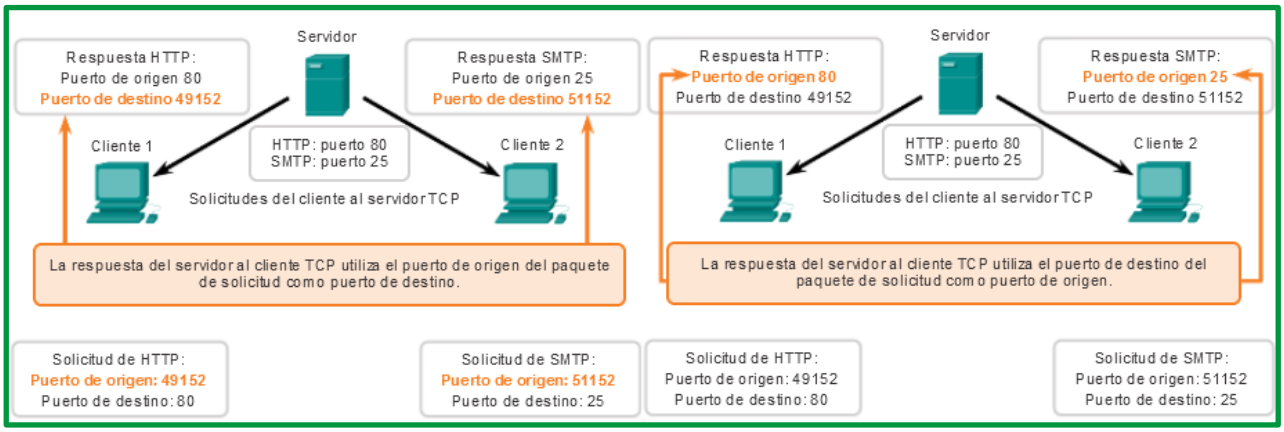


Figure 19. Respuesta de puertos destino y de puertos de origen

En algunas culturas, cuando dos personas se conocen, generalmente se saludan dándose la mano. Ambas culturas entienden el acto de darse la mano como señal de un saludo amigable. Las conexiones en la red son similares. El primer enlace solicita la sincronización. El segundo enlace acusa recibo de la solicitud de sincronización inicial y sincroniza los parámetros de conexión en la dirección opuesta. El tercer segmento de enlace es un acuse de recibo que se utiliza para informarle al destino que ambos lados están de acuerdo en que se estableció una conexión.

Cuando dos hosts se comunican utilizando TCP, se establece una conexión antes de que puedan intercambiarse los datos. Luego de que se completa la comunicación, se cierran las sesiones y la conexión finaliza. Los mecanismos de conexión y sesión habilitan la función de confiabilidad de TCP. Vea en la figura los pasos para establecer y terminar una conexión del TCP.

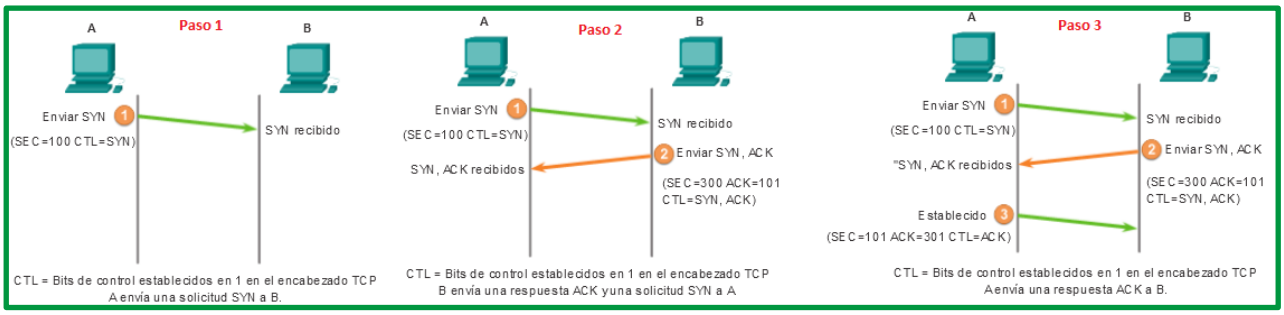


Figure 20. Establecimiento de una comunicación TCP.

Los hosts hacen un seguimiento de cada segmento de datos dentro de una sesión e intercambian información sobre qué datos se reciben mediante la información del encabezado TCP. TCP es un protocolo full-duplex, en el que cada conexión representa dos streams de comunicación unidireccionales, o sesiones. Para establecer la conexión los hosts realizan un protocolo de enlace de tres vías. Los bits de control en el encabezado TCP indican el progreso y estado de la conexión. Enlace de tres vías:

- Establece que el dispositivo de destino se presente en la red.
- Verifica que el dispositivo de destino tenga un servicio activo y que acepte solicitudes en el número de puerto de destino que el cliente de origen intenta utilizar para la sesión.
- Informa al dispositivo de destino que el cliente de origen intenta establecer una sesión de comunicación en dicho número de puerto

En las conexiones TCP, el cliente del host establece la conexión con el servidor. Los tres pasos en el establecimiento de una conexión TCP son:

- ***Paso 1***. El cliente de origen solicita una sesión de comunicación de cliente a servidor con el servidor.
- ***Paso 2***. El servidor acusa recibo de la sesión de comunicación de cliente a servidor y solicita una sesión de comunicación de servidor a cliente.
- ***Paso 3***. El cliente de origen acusa recibo de la sesión de comunicación de servidor a cliente.

Para comprender el proceso de enlace de tres vías, observe los diversos valores que intercambian ambos hosts. Dentro del encabezado del segmento TCP, existen seis campos de 1 bit que contienen información de control utilizada para gestionar los procesos de TCP. Estos campos son los siguientes:

- **URG**: campo indicador urgente importante
- **ACK**: campo de acuse de recibo importante
- **PSH**: función de empuje
- **RST**: restablecer la conexión
- **SYN**: sincronizar números de secuencia
- **FIN**: no hay más datos del emisor

Los campos ACK y SYN son importantes para el análisis del protocolo de enlace de tres vías.

Mediante el resultado del software de análisis de protocolos, como los resultados de Wireshark, se puede examinar la operación del protocolo TCP de enlace de tres vías:

Paso 1: El cliente de origen solicita una sesión de comunicación de cliente a servidor con el servidor.

Un cliente TCP inicia un protocolo de enlace de tres vías al enviar un segmento con el indicador de control de sincronizar números de secuencia (SYN) establecido, lo que indica un valor inicial en el campo de número de secuencia en el encabezado. Este valor inicial para el número de secuencia, conocido como número de secuencia inicial (ISN), se elige de manera aleatoria y se utiliza para comenzar a rastrear el flujo de datos de esta sesión desde el cliente hasta el servidor. El ISN en el encabezado de cada segmento se incrementa en uno por cada byte de datos enviados desde el cliente hacia el servidor mientras continúa la conversación de datos.

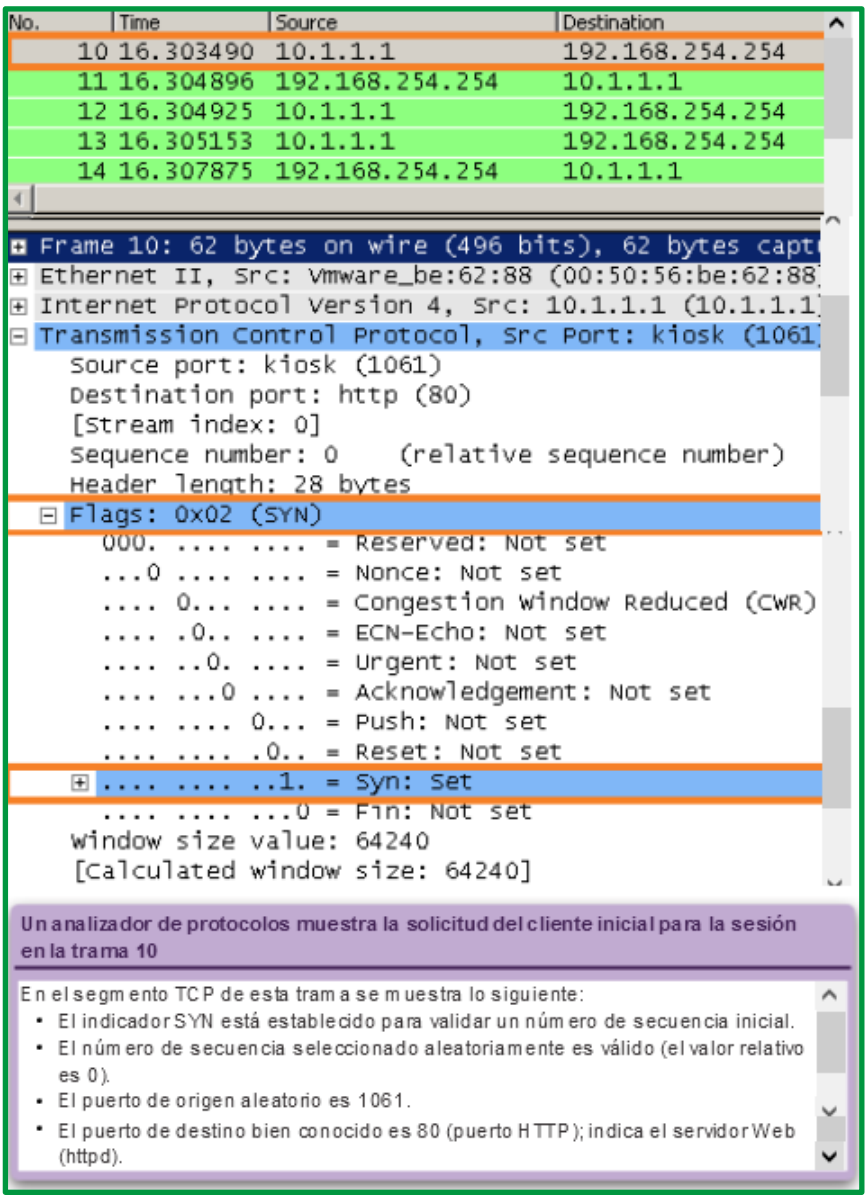


Figure 21. protocolo de enlace de tres vías (SYN)

Como se muestra en la figura, el resultado de un analizador de protocolos muestra el señalizador de control SYN y el número de secuencia relativa. El indicador de control SYN está establecido y el número de secuencia relativa está en 0. Aunque el analizador de protocolos en el gráfico indique los valores relativos para los números de secuencia y de acuse de recibo, los verdaderos valores son números binarios de 32 bits. En la ilustración, se muestran los cuatro bytes representados en un valor hexadecimal.

Paso 2: El servidor reconoce la sesión de comunicación de cliente a servidor y solicita una sesión de comunicación de servidor a cliente.

El servidor TCP debe dar acuse de recibo del segmento SYN del cliente para establecer la sesión de cliente a servidor. Para hacerlo, el servidor envía un segmento al cliente con el indicador de acuse de recibo (ACK) establecido que indica que el número de acuse de recibo es significativo. Con este señalizador establecido en el segmento, el cliente interpreta esto como acuse de recibo de que el servidor ha recibido el SYN del cliente TCP.

El valor del campo de número de acuse de recibo es igual al ISN más 1. Esto establece una sesión del cliente al servidor. El indicador ACK permanece establecido para mantener el equilibrio de la sesión. Recuerde que la conversación entre el cliente y el servidor son, en realidad, dos sesiones unidireccionales: una del cliente al servidor y otra del servidor al cliente. En este segundo paso del protocolo de enlace de tres vías, el servidor debe iniciar la respuesta al cliente. Para comenzar esta sesión, el servidor utiliza el señalizador SYN de la misma manera en que lo hizo el cliente. Establece el señalizador de control SYN en el encabezado para establecer una sesión del servidor al cliente. El señalizador SYN indica que el valor inicial del campo de número de secuencia se encuentra en el encabezado. Este valor se utiliza para hacer un seguimiento del flujo de datos en esta sesión del servidor al cliente.

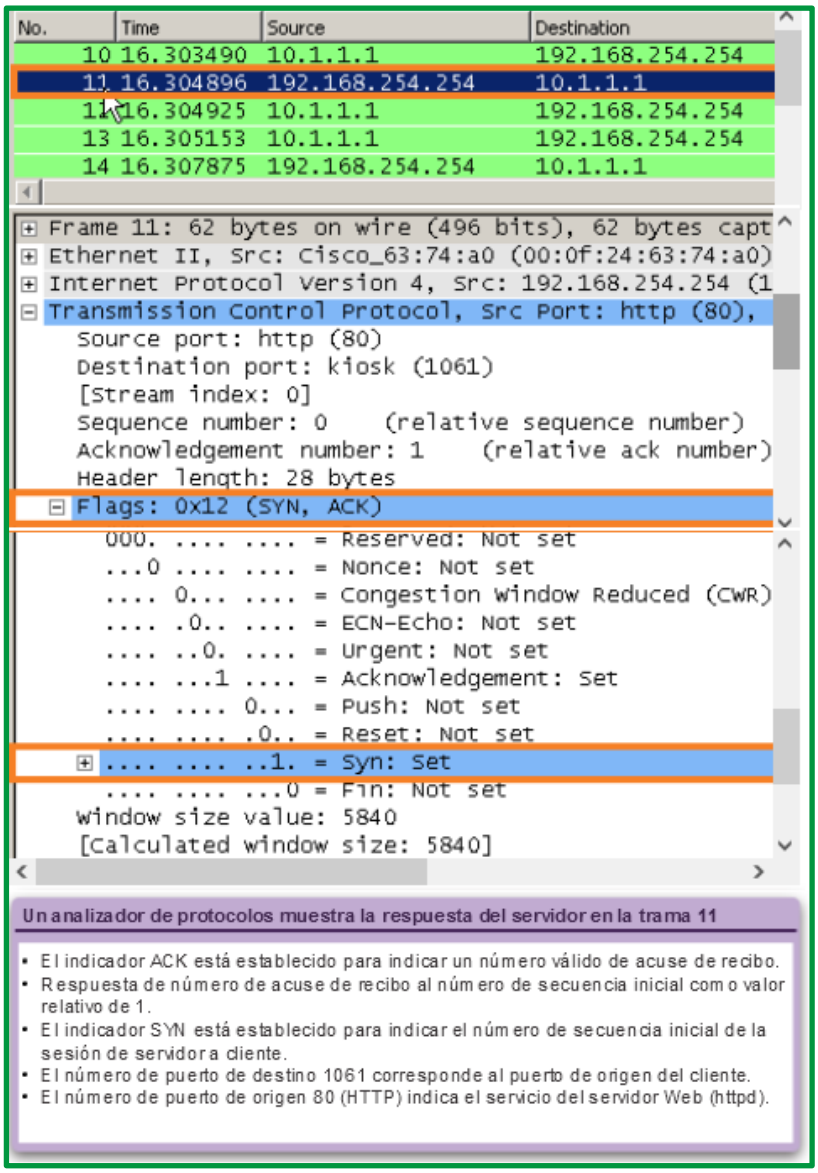


Figure 22. Protocolo TCP de enlace de tres vías (ACK y SYN)

Como se muestra en la ilustración, el resultado del analizador de protocolos muestra que se establecieron los indicadores de control ACK y SYN y que se muestran los números de acuse de recibo y de secuencia relativa.

Paso 3: El cliente de origen reconoce la sesión de comunicación de servidor a cliente.

Por último, el cliente TCP responde con un segmento que contiene un ACK que actúa como respuesta al SYN de TCP enviado por el servidor. No existen datos de usuario en este segmento. El valor del campo de número de acuse de recibo contiene uno más que el ISN recibido del servidor. Una vez que se establecen ambas sesiones entre el cliente y el servidor, todos los segmentos adicionales que se intercambian en esta comunicación tendrán establecido el indicador ACK.

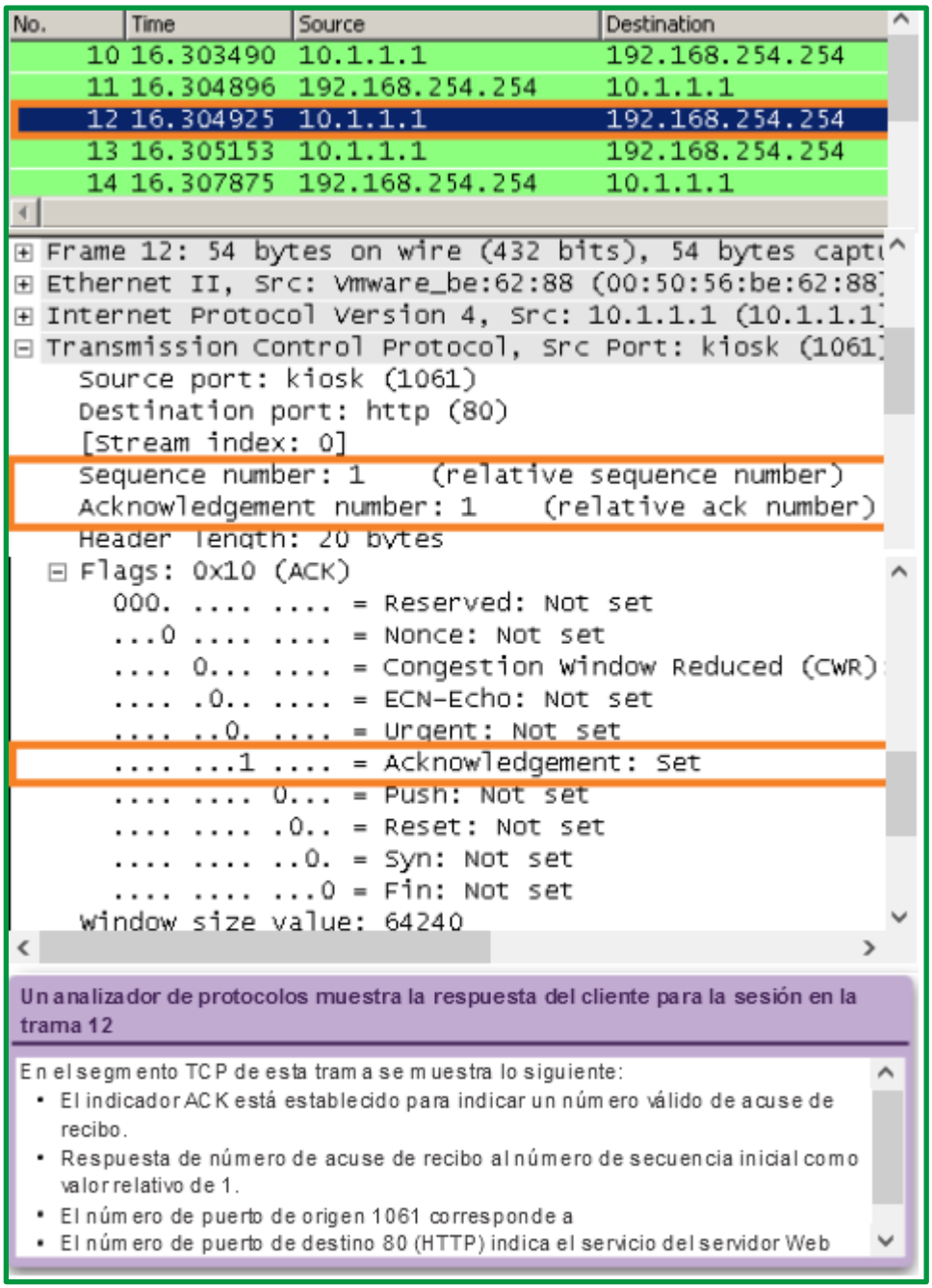


Figure 23. ACK establecido, números de acuse de recibo y secuencia relativa

Como se muestra en la ilustración, el resultado del analizador de protocolos muestra el indicador de control ACK establecido y los números de acuse de recibo y de secuencia relativa. Se puede añadir seguridad a la red de datos de la siguiente manera:

- Denegar el establecimiento de sesiones del TCP.
- Permitir sólo sesiones que se establezcan para servicios específicos.
- Permitir sólo tráfico como parte de sesiones ya establecidas.

Estas medidas de seguridad se pueden implementar para todas las sesiones TCP o solo para las sesiones seleccionadas.

Liberación de una conexión

Para cerrar una conexión, se debe establecer el indicador de control finalizar (FIN) en el encabezado del segmento. Para finalizar todas las sesiones TCP de una vía, se utiliza un enlace de dos vías, que consta de un segmento FIN y un segmento ACK. Por lo tanto, para terminar una única conversación que admite TCP, se requieren cuatro intercambios para finalizar ambas sesiones, como se muestra en la figura siguiente.

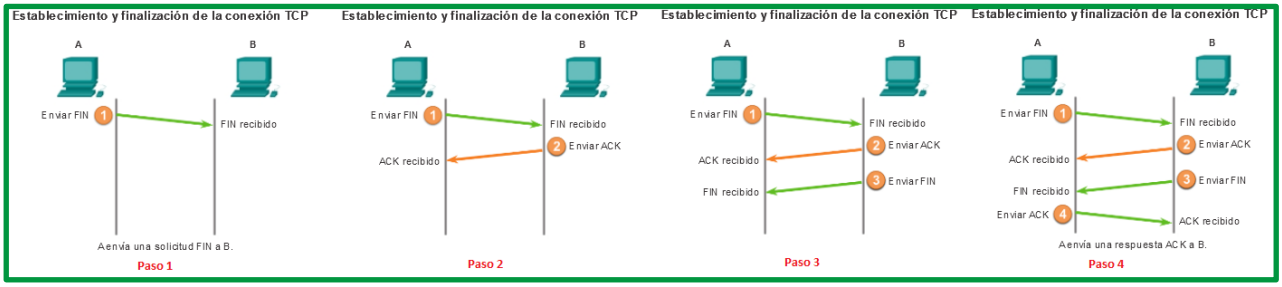


Figure 24. Finalización de la Conexión TCP

Nota: En esta explicación, los términos “cliente” y “servidor” se utilizan como referencia con fines de simplificación, pero el proceso de finalización lo pueden iniciar dos hosts cualesquiera que tengan una sesión abierta:

- **Paso 1**: cuando el cliente no tiene más datos para enviar en el stream, envía un segmento con el indicador FIN establecido.
- **Paso 2**: el servidor envía un ACK para acusar recibo del FIN y terminar la sesión de cliente a servidor.
- **Paso 3**: el servidor envía un FIN al cliente para terminar la sesión de servidor a cliente.
- **Paso 4**: el cliente responde con un ACK para dar acuse de recibo del FIN desde el servidor.

Cuando el cliente no tiene más datos que transferir, establece el indicador FIN en el encabezado de un segmento. A continuación, el extremo servidor de la conexión envía un segmento normal que contiene datos con el indicador ACK establecido utilizando el número de acuse de recibo, lo que confirma que se recibieron todos los bytes de datos. Cuando se dio acuse de recibo de todos los segmentos, la sesión se cierra.

La sesión en la otra dirección se cierra con el mismo proceso. El receptor indica que no existen más datos para enviar estableciendo el señalizador **FIN** en el encabezado del segmento enviado al origen. Un acuse de recibo devuelto confirma que todos los bytes de datos se recibieron y que la sesión, a su vez, finalizó.

Analice la figura siguiente para ver los indicadores de control FIN y ACK establecidos en el encabezado del segmento, lo que finaliza la sesión HTTP.

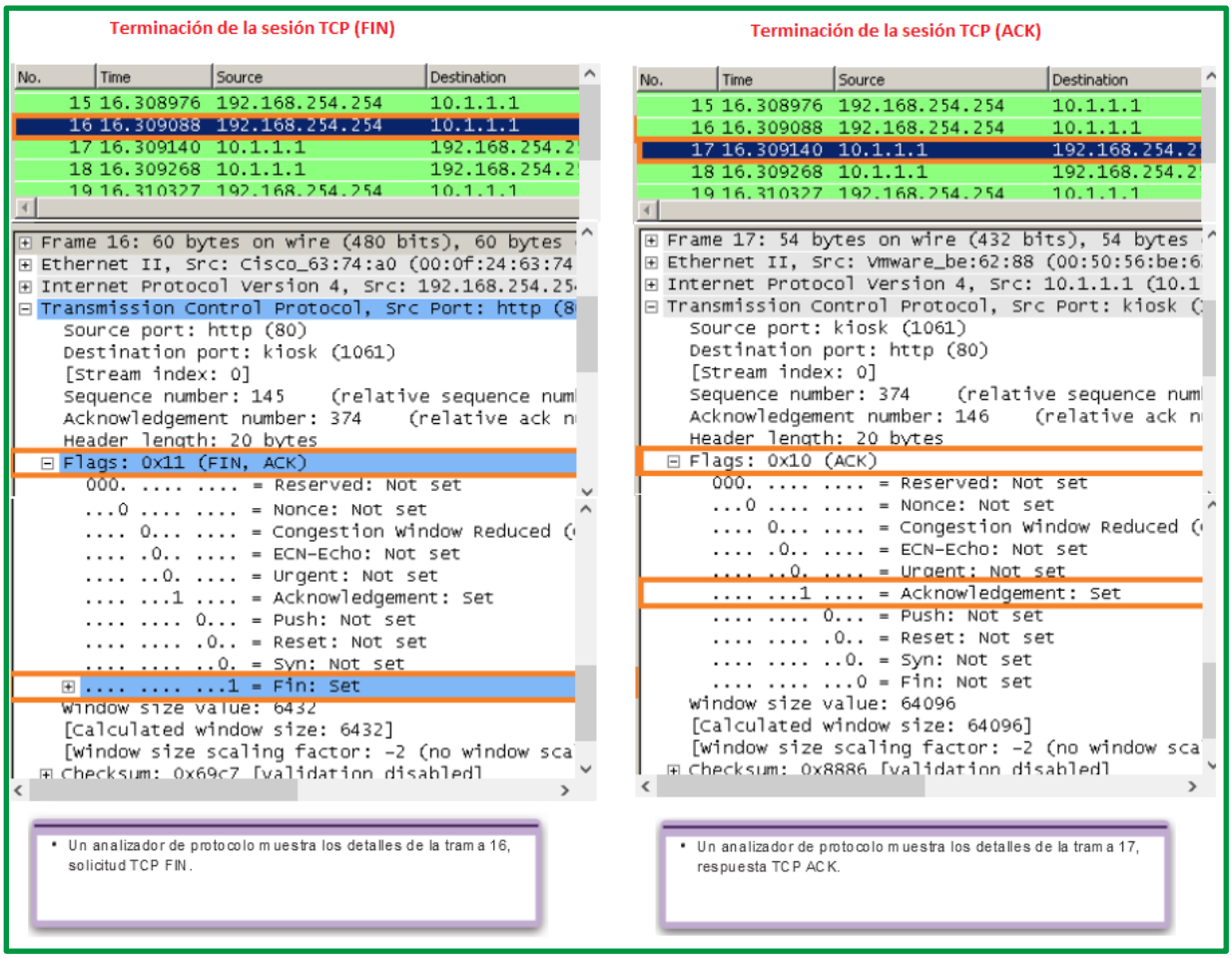


Figure 25. Terminación de comunicación TCP

También es posible terminar la conexión por medio de un enlace de tres vías. Cuando el cliente no posee más datos para enviar, envía un señalizador FIN al servidor. Si el servidor tampoco tiene más datos para enviar, puede responder con los señalizadores FIN y ACK, combinando dos pasos en uno. A continuación, el cliente responde con un ACK.

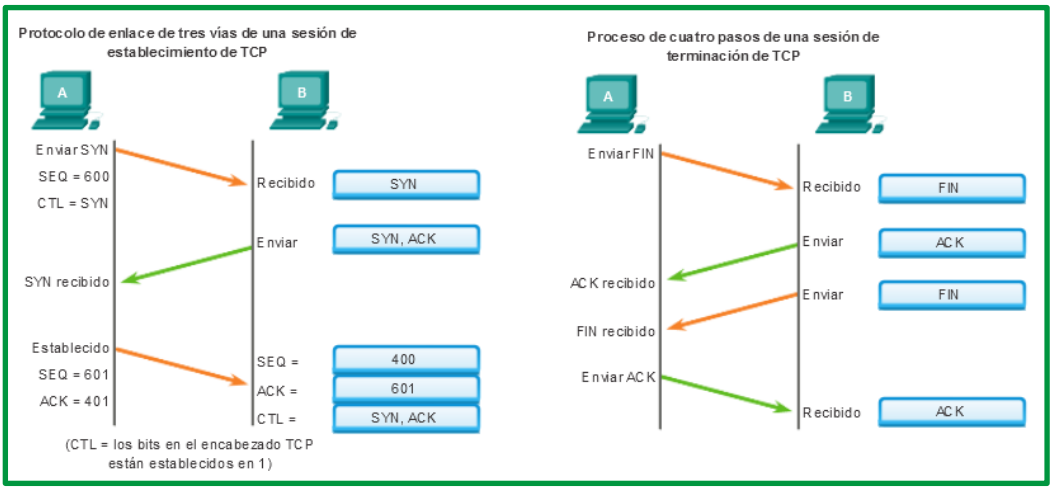


Figure 26. Proceso de establecimiento de comunicaciones y terminación en TCP

Control de flujo y almacenamiento de buffer

Reordenamiento de segmentos

Cuando los servicios envían datos mediante el TCP, los segmentos pueden llegar a su destino en desorden. Para que el receptor comprenda el mensaje original, los datos en estos segmentos se reensamblan en el orden original. Para lograr esto, se asignan números de secuencia en el encabezado de cada paquete.

Durante la configuración de la sesión, se establece un número de secuencia inicial (ISN). Este ISN representa el valor inicial para los bytes para esta sesión que se transmite a la aplicación receptora. A medida que se transmiten los datos durante la sesión, el número de secuencia se incrementa en el número de bytes que se han transmitido. Este seguimiento de bytes de datos permite identificar y dar acuse de recibo de cada segmento de manera exclusiva. Se pueden identificar segmentos perdidos.

Los números de secuencia de segmento habilitan la confiabilidad al indicar cómo rearmar y reordenar los segmentos recibidos, como se muestra en la ilustración.

El proceso TCP receptor coloca los datos del segmento en un búfer de recepción. Los segmentos se colocan en el orden de número de secuencia correcto y se pasan a la capa de aplicación cuando se rearman. Todos los segmentos que llegan con números de secuencia no contiguos se mantienen para su posterior procesamiento. A continuación, cuando llegan los segmentos con bytes faltantes, tales segmentos se procesan en orden.

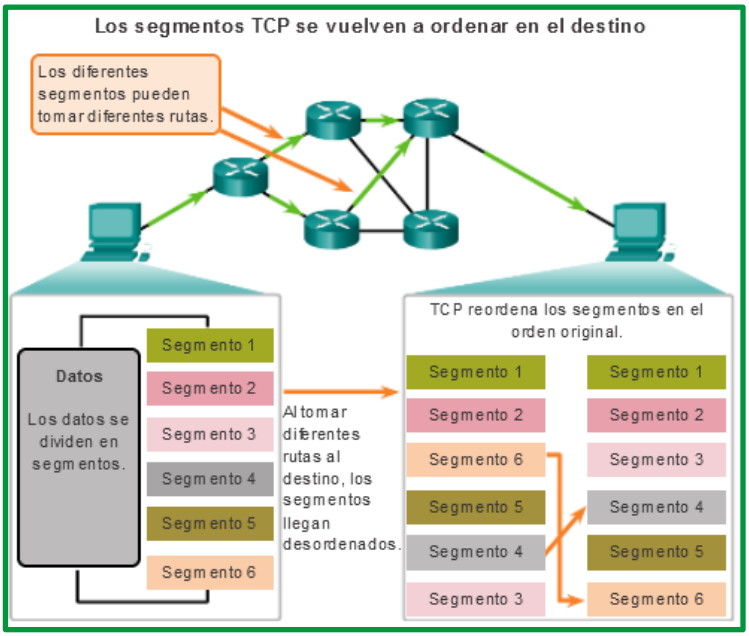


Figure 27. Segmentos en TCP

Confirmación de recepción de segmentos

Una de las funciones de TCP es garantizar que cada segmento llegue a destino. Los servicios de TCP en el host de destino envían un acuse de recibo de los datos que recibe la aplicación de origen.

El número de secuencia (SEQ) y el número de acuse de recibo (ACK) se utilizan juntos para confirmar la recepción de los bytes de datos contenidos en los segmentos transmitidos. El número de SEQ indica la cantidad relativa de bytes que se transmitieron en esta sesión, incluso

los bytes en el segmento actual. TCP utiliza el número de ACK reenviado al origen para indicar el próximo byte que el receptor espera recibir. Esto se llama acuse de recibo de expectativa.

Se le informa al origen que el destino recibió todos los bytes de este stream de datos, hasta el byte especificado por el número de ACK, pero sin incluirlo. Se espera que el host emisor envíe un segmento que utiliza un número de secuencia que es igual al número de ACK.

Recuerde que cada conexión son realmente dos sesiones de una vía. Los números de SEQ y ACK se intercambian en ambas direcciones.

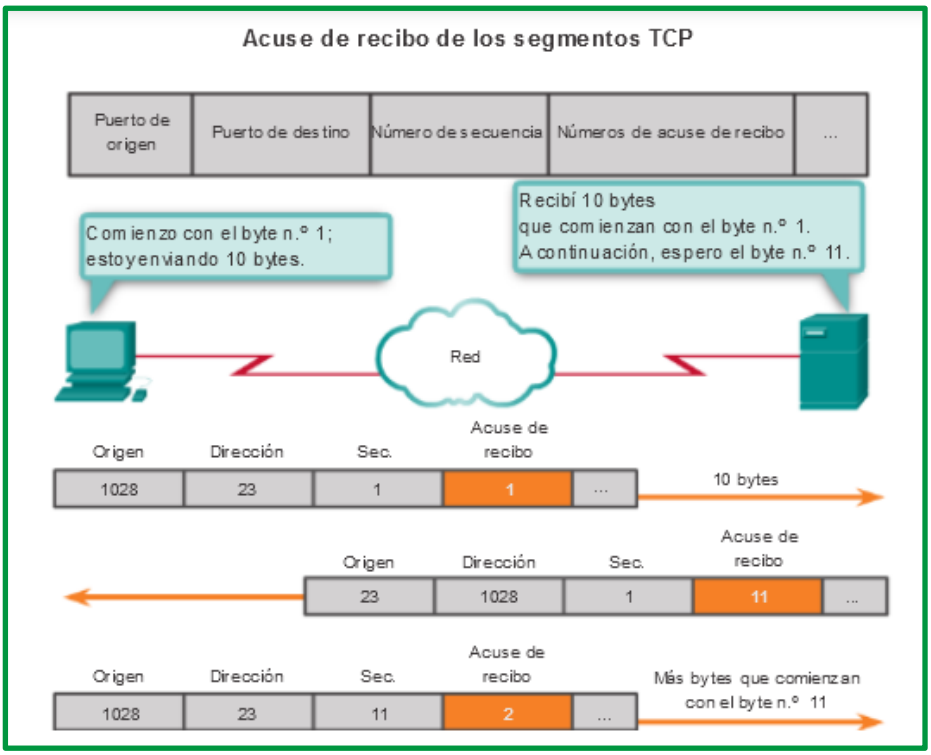


Figure 28. Acuse de recibo de segmentos TCP

En el ejemplo de la figura, el host de la izquierda envía datos al host de la derecha. Envía un segmento que contiene 10 bytes de datos para esta sesión y un número de secuencia igual a 1 en el encabezado.

El host receptor recibe el segmento en la capa 4 y determina que el número de secuencia es 1 y que tiene 10 bytes de datos. Luego el host envía un segmento de vuelta al host de la izquierda para acusar recibo de estos datos. En este segmento, el host establece el número de ACK en 11 para indicar que el siguiente byte de datos que espera recibir en esta sesión es el byte número 11. Cuando el host emisor recibe este acuse de recibo, puede enviar el próximo segmento que contiene datos para esta sesión a partir del byte 11.

En este ejemplo, si el host emisor tuviera que esperar el acuse de recibo de cada uno de los 10 bytes, la red tendría mucha sobrecarga. Para reducir la sobrecarga de estos acuses de recibo, pueden enviarse varios segmentos de datos y dar acuse de recibo de estos con un único mensaje de TCP en la dirección opuesta. Este acuse de recibo contiene un número de ACK que se basa en la cantidad total de bytes recibidos en la sesión. Por ejemplo, si se comienza con un número de

secuencia 2000, si se reciben 10 segmentos de 1000 bytes cada uno, se devolverá al origen un número de ACK igual a 12 001.

La cantidad de datos que un origen puede transmitir antes de recibir un acuse de recibo se denomina “tamaño de la ventana”, que es un campo en el encabezado TCP que permite administrar datos perdidos y controlar el flujo.

Manejo de segmentos perdidos

La pérdida de datos se produce en ocasiones, sin importar qué tan bien diseñada esté la red; por lo tanto, TCP proporciona métodos para administrar estas pérdidas de segmentos. Entre estos está un mecanismo para retransmitir segmentos con datos sin acuse de recibo.

Un servicio de host de destino que utiliza TCP generalmente sólo da acuse de recibo de datos para bytes de secuencia continuos. Si faltan uno o más segmentos, solo se hace acuse de recibo de los datos en la primera secuencia contigua de bytes. Por ejemplo, si se reciben segmentos con números de secuencia de 1500 a 3000 y de 3400 a 3500, el número de ACK sería 3001. Esto se debe a que hay segmentos con números de SEQ de 3001 a 3399 que no se recibieron.

Cuando el TCP en el host de origen no recibe un acuse de recibo después de una cantidad de tiempo predeterminada, este vuelve al último número de ACK recibido y vuelve a transmitir los datos desde ese punto en adelante. La solicitud de comentarios (RFC) no especifica el proceso de retransmisión, pero se deja a criterio de la implementación particular del TCP.

Para una implementación de TCP típica, un host puede transmitir un segmento, colocar una copia del segmento en una cola de retransmisión e iniciar un temporizador. Cuando se recibe el acuse de recibo de los datos, se elimina el segmento de la cola. Si no se recibe el acuse de recibo antes de que el temporizador venza, el segmento es retransmitido.

En la actualidad, los hosts pueden emplear también una característica optativa llamada “acuses de recibo selectivos” (SACK). Si ambos hosts admiten los SACK, es posible que el destino acuse recibo de los bytes de segmentos discontinuos, y el host solo necesitará volver a transmitir los datos perdidos.

Control de flujo

TCP también proporciona mecanismos para el control del flujo. El control del flujo permite mantener la confiabilidad de la transmisión de TCP mediante el ajuste de la velocidad del flujo de datos entre el origen y el destino para una sesión dada. El control del flujo se logra limitando la cantidad de segmentos de datos que se envían al mismo tiempo y solicitando acuses de recibo antes de enviar más segmentos.

Para lograr el control del flujo, lo primero que determina TCP es la cantidad de segmentos de datos que puede aceptar el dispositivo de destino. El encabezado TCP incluye un campo de 16 bits llamado “***tamaño de la ventana***”. Esta es la cantidad de bytes que el dispositivo de destino de una sesión TCP puede aceptar y procesar al mismo tiempo. El tamaño inicial de la ventana se acuerda durante el inicio de sesión entre el origen y el destino por medio del protocolo de enlace de tres vías. Una vez acordado el tamaño, el dispositivo de origen debe limitar la cantidad de segmentos de datos enviados al dispositivo de destino sobre la base del tamaño de la ventana. El

dispositivo de origen puede continuar enviando más datos para la sesión solo cuando obtiene un acuse de recibo de los segmentos de datos recibidos.

Durante el retraso en la recepción del acuse de recibo, el emisor no envía ningún otro segmento. En los períodos en los que la red está congestionada o los recursos del host receptor están exigidos, la demora puede aumentar. A medida que aumenta esta demora, disminuye la tasa de transmisión efectiva de los datos para esta sesión. La disminución de velocidad en la transmisión de datos de cada sesión ayuda a reducir el conflicto de recursos en la red y en el dispositivo de destino cuando se ejecutan varias sesiones.

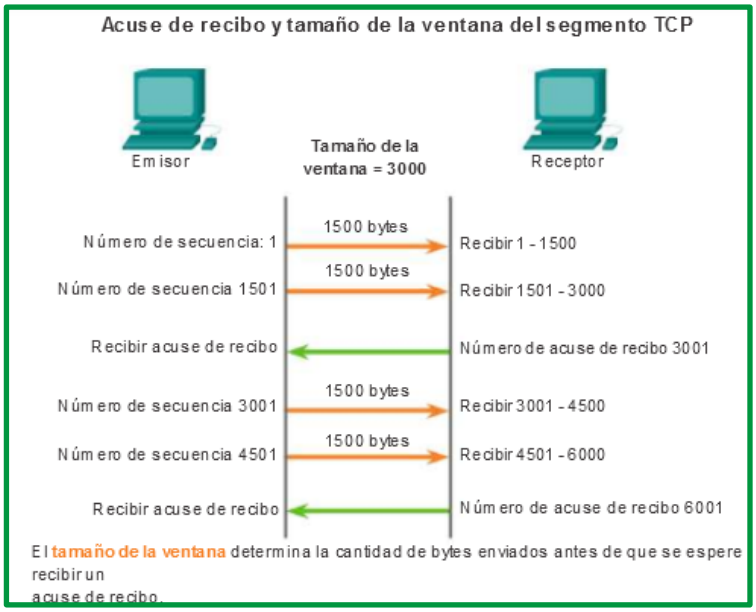


Figure 29. Tamaño de ventana y acuse de recibo

Ver la figura para obtener una representación simplificada del tamaño de la ventana y los acuses de recibo. En este ejemplo, el tamaño de la ventana inicial para una sesión TCP representada se establece en 3000 bytes. Cuando el emisor transmite 3000 bytes, espera por un acuse de recibo de los mismos antes de transmitir más segmentos para esta sesión. Una vez que el emisor obtiene este acuse de recibo del receptor, puede transmitir 3000 bytes adicionales.

TCP utiliza tamaños de ventana para tratar de aumentar la velocidad de transmisión hasta el flujo máximo que la red y el dispositivo de destino pueden admitir y, al mismo tiempo, minimizar las pérdidas y las retransmisiones.

Reducción del tamaño de la ventana

Otra forma de controlar el flujo de datos es utilizar tamaños de ventana dinámicos. Cuando los recursos de la red son limitados, TCP puede reducir el tamaño de la ventana para lograr que los segmentos recibidos sean reconocidos con mayor frecuencia. Esto reduce de forma efectiva la velocidad de transmisión porque el origen espera que se dé acuse de recibo de los datos con más frecuencia.

El host receptor envía el valor del tamaño de la ventana al host emisor para indicar la cantidad de bytes que puede recibir. Si el destino necesita disminuir la velocidad de comunicación debido,

por ejemplo, a una memoria de búfer limitada, puede enviar un valor más pequeño del tamaño de la ventana al origen como parte del acuse de recibo.

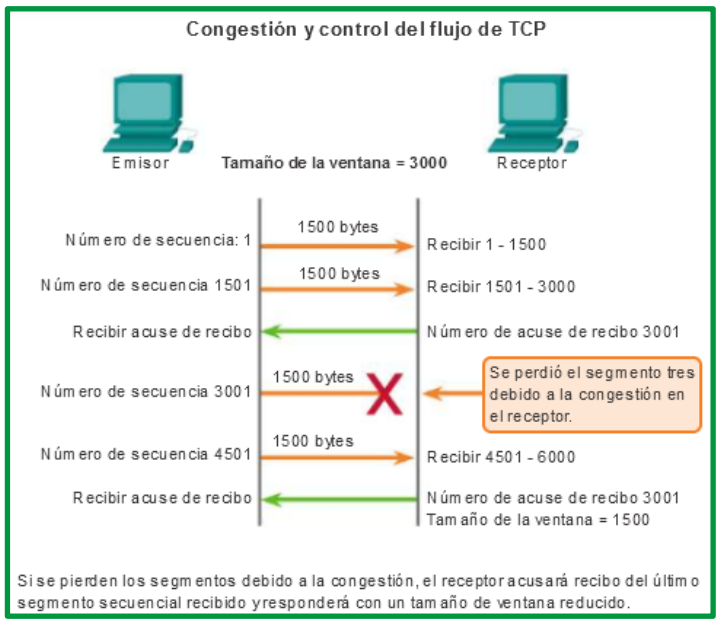


Figure 30. Congestión y perdida de segmentos TCP

Como se muestra en la ilustración, si un host receptor está congestionado, puede responder al host emisor con un segmento que especifique un tamaño reducido de la ventana. En esta ilustración, se muestra que se produjo la pérdida de uno de los segmentos. El receptor cambió el campo de la ventana en el encabezado TCP de los segmentos devueltos en esta conversación de 3000 a 1500. Esto hizo que el emisor redujera el tamaño de la ventana a 1500.

Después de un período de transmisión sin pérdidas de datos ni recursos limitados, el receptor comienza a aumentar el campo de la ventana, lo que reduce la sobrecarga en la red, ya que se deben enviar menos acuses de recibo. El tamaño de la ventana sigue aumentando hasta que se produce la pérdida de datos, lo que provoca que disminuya el tamaño de la ventana.

Este aumento y disminución dinámicos del tamaño de la ventana es un proceso continuo en TCP. En redes altamente eficaces, los tamaños de la ventana pueden ser muy grandes, porque no se pierden datos. En redes en las que la infraestructura subyacente está bajo presión, es probable que el tamaño de la ventana se mantenga pequeño.

Multiplexión y demultiplexación

En el host de destino, la capa de transporte recibe segmentos procedentes de la capa de red que tiene justo debajo. La capa de transporte tiene la responsabilidad de entregar los datos contenidos en estos segmentos al proceso de la aplicación apropiada que está ejecutándose en el host. Veamos un ejemplo. Suponga que está sentado frente a su computadora y que está descargando páginas web a la vez que ejecuta una sesión FTP y dos sesiones Telnet. Por tanto, tiene cuatro procesos de aplicación de red en ejecución: dos procesos Telnet, un proceso FTP y un proceso HTTP. Cuando la capa de transporte de su computadora recibe datos procedentes de la capa de red, tiene que dirigir los datos recibidos a uno de estos cuatro procesos.

En primer lugar, recordemos que un proceso puede tener uno o más sockets, puertas por las que pasan los datos de la red al proceso, y viceversa.

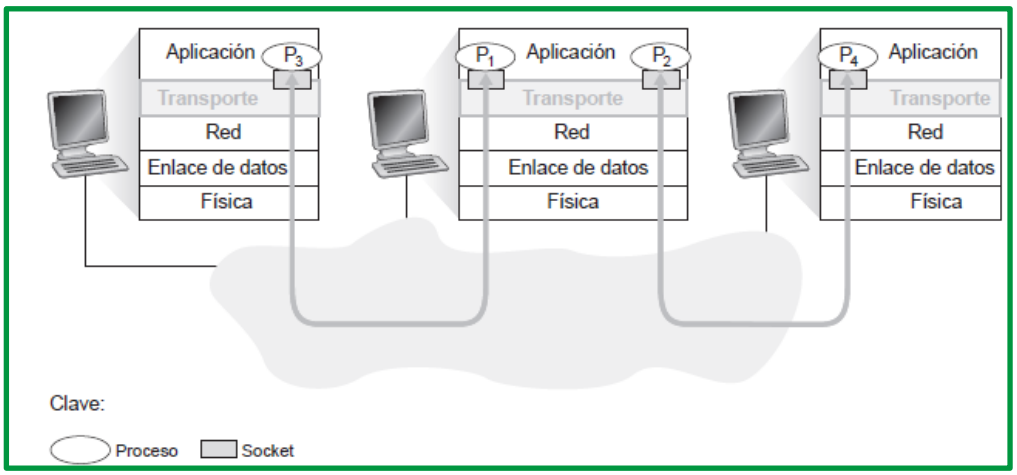


Figure 31. Multiplexación y demultiplexación capa de transporte.
Fuente: Libro Redes de computadoras. Un enfoque descendente, 7 Edición

Por tanto, como se muestra en la ilustración, la capa de transporte del host receptor realmente no entrega los datos directamente a un proceso, sino a un socket intermedio. Dado que en cualquier instante puede haber más de un socket en el host receptor, cada socket tiene asociado un identificador único. El formato de este identificador depende de si se trata de un socket UDP o de un socket TCP.

Cada segmento de la capa de transporte contiene un conjunto de campos destinados a este propósito. En el extremo receptor, la capa de transporte examina estos campos para identificar el socket receptor y, a continuación, envía el segmento a dicho socket. Esta tarea de entregar los datos contenidos en un segmento de la capa de transporte al socket correcto es lo que se denomina ***demultiplexación***. La tarea de reunir los fragmentos de datos en el host de origen desde los diferentes sockets, encapsulando cada fragmento de datos con la información de cabecera (la cual se utilizará después en el proceso de demultiplexación) para crear los segmentos y pasarlos a la capa de red es lo que se denomina ***multiplexación***.

Observe que la capa de transporte del host intermedio de la ilustración tiene que demultiplexar los segmentos que llegan de la capa de red inferior para entregárselos a los procesos P1 o P2 de la capa superior; esto se hace dirigiendo los datos del segmento entrante al correspondiente socket del proceso. La capa de transporte del host intermedio también tiene que recopilar los datos salientes desde estos sockets, construir los segmentos de la capa de transporte y pasar dichos segmentos a la capa de red. Aunque hemos presentado la multiplexación y la demultiplexación en el contexto de los protocolos de transporte de Internet, es importante darse cuenta de que esas técnicas son necesarias siempre que un único protocolo en una capa (en la capa de transporte o cualquier otra) sea utilizado por varios protocolos de la capa inmediatamente superior.

Basándonos en las explicaciones anteriores, sabemos que la operación de multiplexación que se lleva a cabo en la capa de transporte requiere (1) que los sockets tengan identificadores únicos y

(2) que cada segmento tenga campos especiales que indiquen el socket al que tiene que entregarse el segmento. Estos campos especiales, son el campo ***número de puerto de origen*** y el campo ***número de puerto de destino***. Cada número de puerto es un número de 16 bits comprendido en el rango de 0 a 65535. Los números de puerto pertenecientes al ***rango de 0 a 1023*** se conocen como ***números de puertos bien conocidos*** y son restringidos, lo que significa que están reservados para ser empleados por los protocolos de aplicación bien conocidos, como por ejemplo HTTP (que utiliza el número de puerto 80) y FTP (que utiliza el número de puerto 21). Puede encontrar la lista de números de puerto bien conocidos en el documento RFC 1700 y su actualización en la dirección http://www.iana.org [RFC 3232]. Al desarrollar una nueva aplicación, es necesario asignar un número de puerto a la aplicación.

La capa de transporte podría implementar el servicio de demultiplexación: cada socket del host se puede asignar a un número de puerto y, al llegar un segmento al host, la capa de transporte examina el número de puerto de destino contenido en el segmento y lo envía al socket correspondiente. A continuación, los datos del segmento pasan a través del socket y se entregan al proceso asociado. Como veremos, esto es básicamente lo que hace UDP. Sin embargo, también conocemos que la tarea de multiplexación/demultiplexación en TCP es más sutil.

A nivel de la capa de transporte se pueden encontrar multiplexación y demultiplexación sin conexión y orientadas a la conexión.

Multiplexación y demultiplexación sin conexión: Orientados a los protocolos UDP, un socket UDP queda completamente identificado por una tupla que consta de ***una dirección IP de destino*** y ***un número de puerto de destino***.; con lo cual, si dos segmentos UDP tienen diferentes direcciones IP y/o números de puerto de origen, pero la misma dirección IP de destino y el mismo número puerto de destino, entonces los dos segmentos se enviarán al mismo proceso de destino a través del mismo socket de destino.

Multiplexación y demultiplexación orientadas a la conexión: Aplicadas en el protocolo TCP, una diferencia entre el socket TCP y un socket UDP es que el primero queda identificado por una tupla de cuatro elementos: ***dirección IP de origen***, ***número de puerto de origen***, ***dirección IP de destino***, ***número de puerto de destino***. Por tanto, cuando un segmento TCP llega a un host procedente de la red, el host emplea los cuatro valores para dirigir (demultiplexar) el segmento al socket apropiado. En particular, y al contrario de lo que ocurre con UDP, dos segmentos TCP entrantes con direcciones IP de origen o números de puerto de origen diferentes (con la excepción de un segmento TCP que transporte la solicitud original de establecimiento de conexión) serán dirigidos a dos sockets distintos.

En la ilustración siguiente se observa que el ***host C*** inicia dos sesiones HTTP con el servidor B y el ***host A*** inicia una sesión HTTP también con B. Los hosts A y C y el servidor B tienen sus propias direcciones IP únicas (A, C y B, respectivamente). ***El host C*** asigna dos números de puerto de origen diferentes (26145 y 7532) a sus dos conexiones HTTP. Dado que el host A está seleccionando los números de puerto de origen independientemente de C, también puede asignar el número de puerto de origen 26145 a su conexión HTTP. Pero esto no es un problema: el servidor B todavía podrá demultiplexar correctamente las dos conexiones con el mismo número de puerto de origen, ya que tienen direcciones IP de origen diferentes.

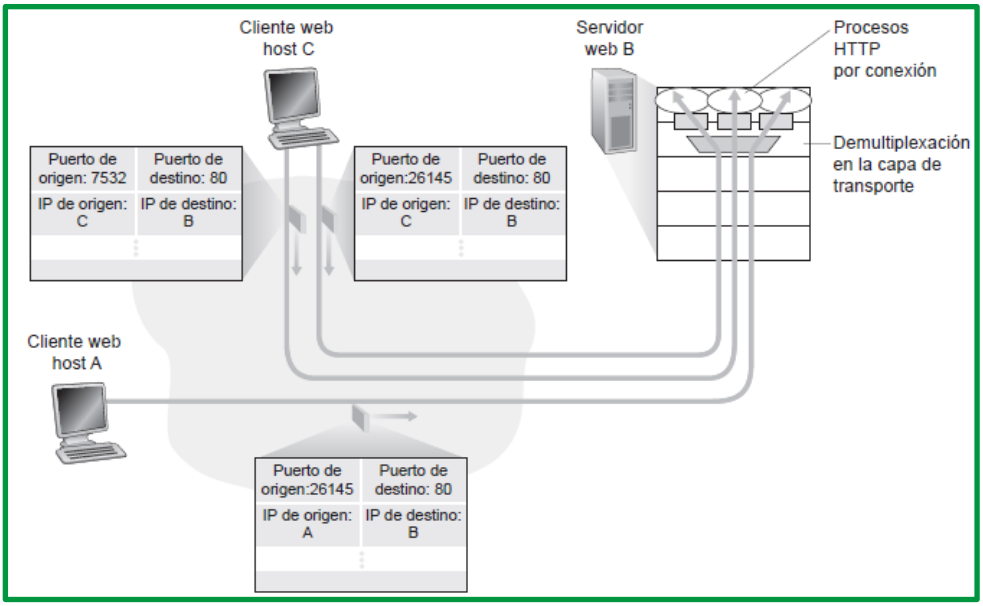


Figure 32. Dos clientes utilizando el mismo número de puerto de destino para comunicarse con el mismo servidor web
Fuente: Libro Redes de computadoras. Un enfoque descendente, 7 Edición

Protocolos de transporte de internet: TCP.

Como se indicó anteriormente, TCP se considera un protocolo de transporte confiable, lo que significa que incluye procesos para garantizar la entrega confiable entre aplicaciones mediante el uso de entrega con acuse de recibo. La función del protocolo de transporte TCP es similar al envío de paquetes de los que se hace un seguimiento de origen a destino. Si se divide un pedido de FedEx en varios envíos, el cliente puede revisar en línea el orden de la entrega.

Con TCP, las tres operaciones básicas de confiabilidad son las siguientes:

- Seguimiento de segmentos de datos transmitidos
- Acuse de recibo de datos.
- Retransmisión de cualquier dato sin acuse de recibo.

TCP divide el mensaje en partes pequeñas, conocidas como segmentos. Los segmentos se numeran en secuencia y se pasan al proceso IP para armarse en paquetes. TCP realiza un seguimiento del número de segmentos que se enviaron a un host específico desde una aplicación específica. Si el emisor no recibe un acuse de recibo antes del transcurso de un período determinado, supone que los segmentos se perdieron y los vuelve a transmitir. Sólo se vuelve a enviar la parte del mensaje que se perdió, no todo el mensaje. En el host receptor, TCP se encarga de rearmar los segmentos del mensaje y de pasarlos a la aplicación. El protocolo de transferencia de archivos (FTP) y el protocolo de transferencia de hipertexto (HTTP) son ejemplos de las aplicaciones que utilizan TCP para garantizar la entrega de datos.

Estos procesos de confiabilidad generan una sobrecarga adicional en los recursos de la red debido a los procesos de acuse de recibo, rastreo y retransmisión. Para admitir estos procesos de confiabilidad, se intercambian más datos de control entre los hosts emisores y receptores. Esta información de control está incluida en un encabezado TCP.

TCP se describió inicialmente en RFC 793. Además de admitir funciones básicas de segmentación y rearmado de datos, TCP, también proporciona lo siguiente:

- Conversaciones orientadas a la conexión mediante el establecimiento de sesiones.
- Entrega confiable.
- Reconstrucción de datos ordenada.
- Control del flujo.

Establecimiento de una sesión

TCP es un protocolo orientado a la conexión. Un protocolo orientado a la conexión es uno que negocia y establece una conexión (o sesión) permanente entre los dispositivos de origen y de destino antes de reenviar tráfico. El establecimiento de sesión prepara los dispositivos para que se comuniquen entre sí. Mediante el establecimiento de sesión, los dispositivos negocian la cantidad de tráfico que se puede reenviar en un momento determinado, y los datos que se comunican entre ambos se pueden administrar detenidamente. La sesión se termina solo cuando se completa toda la comunicación.

Entrega confiable

TCP puede implementar un método para garantizar la entrega confiable de los datos. En términos de redes, confiabilidad significa asegurar que cada sección de datos que envía el origen llegue al destino. Por varias razones, es posible que una sección de datos se corrompa o se pierda por completo a medida que se transmite a través de la red. TCP puede asegurar que todas las partes lleguen a destino al hacer que el dispositivo de origen retransmita los datos perdidos o dañados.

Entrega en el mismo orden

Los datos pueden llegar en el orden equivocado, debido a que las redes pueden proporcionar varias rutas que pueden tener diferentes velocidades de transmisión. Al numerar y secuenciar los segmentos, TCP puede asegurar que estos se rearmen en el orden correcto.

Control de flujo

Los hosts de la red cuentan con recursos limitados, como memoria o ancho de banda. Cuando TCP advierte que estos recursos están sobrecargados, puede solicitar que la aplicación emisora reduzca la velocidad del flujo de datos. Esto lo lleva a cabo TCP, que regula la cantidad de datos que transmite el origen. El control de flujo puede evitar la pérdida de segmentos en la red y evitar la necesitad de la retransmisión.

Una vez que TCP establece una sesión, puede hacer un seguimiento de la conversación dentro de esa sesión. Debido a la capacidad de TCP de hacer un seguimiento de conversaciones reales, se lo considera un protocolo con estado. Un protocolo con estado es un protocolo que realiza el seguimiento del estado de la sesión de comunicación. Por ejemplo, cuando se transmiten datos mediante TCP, el emisor espera que el destino acuse recibo de los datos. TCP hace un seguimiento de la información que se envió y de la que se acusó de recibo. Si no se acusa recibo de los datos, el emisor supone que no llegaron y los vuelve a enviar. La sesión con estado

comienza con el establecimiento de sesión y finaliza cuando se cierra la sesión con terminación de sesión.

Recuerde que. - El mantenimiento de esta información de estado requiere recursos que no son necesarios para un protocolo sin estado, como UDP.

TCP genera sobrecarga adicional para obtener estas funciones. Como se muestra en la ilustración, cada segmento TCP tiene 20 bytes de sobrecarga en el encabezado que encapsula los datos de la capa de aplicación. Este tipo de segmento es mucho más largo que un segmento UDP, que solo tiene 8 bytes de sobrecarga.

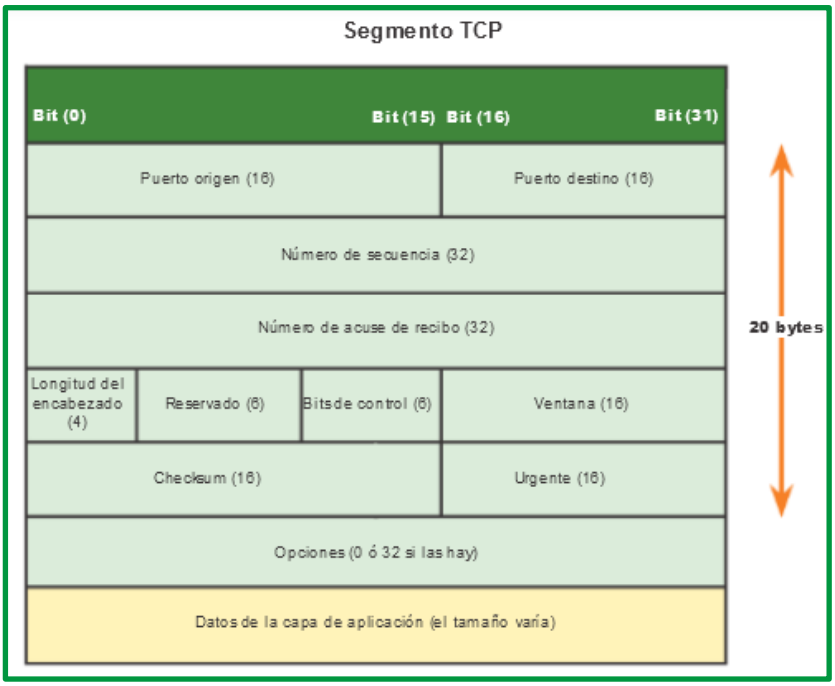


Figure 33. Segmento TCP

La sobrecarga adicional incluye lo siguiente:

- ***Número de secuencia (32 bits)***: Son utilizados por el emisor y el receptor de TCP para implementar un servicio de transferencia de datos fiable, se utiliza para rearmar datos.
- ***Número de acuse de recibo (32 bits)***: Indica los datos que se recibieron.
- ***Longitud del encabezado (4 bits):*** Conocido como "desplazamiento de datos". Indica la longitud del encabezado del segmento TCP.
- ***Reservado (6 bits):*** Este campo está reservado para el futuro.
- ***Bits de control (6 bits):*** Incluye códigos de bit, o indicadores, que indican el propósito y la función del segmento TCP.
- ***Tamaño de la ventana (16 bits):*** Se utiliza para el control de flujo, se emplea para indicar el número de bytes que un receptor está dispuesto a aceptar.
- ***Checksum (16 bits):*** Se utiliza para la verificación de errores en el encabezado y los datos del segmento.

- ***Urgente (16 bits)***: Indica si la información es urgente.
- **Opciones**: Es opcional y de longitud variable. Se utiliza cuando un emisor y un receptor negocian el tamaño máximo de segmento (MSS) o como un factor de escala de la ventana en las redes de alta velocidad. También se define una opción de marca temporal.

Algunos ejemplos de aplicaciones que utilizan TCP son los exploradores Web, el correo electrónico y las transferencias. Se describe la siguiente tabla:

Número de puerto	Aplicación
20	FTP datos
21	FTP control
22	SSH
23	Telnet
25	SMTP
53	DNS
80	HTTP (WWW)
110	POP3
443	SSL

Tabla 1. Aplicaciones que utilizan protocolos TCP

Muchas aplicaciones requieren confiabilidad y otros servicios que proporciona TCP. Estas son aplicaciones que pueden tolerar cierto grado de demora o pérdida de rendimiento debido a la sobrecarga que impone TCP.

Esto hace que TCP sea más adecuado para las aplicaciones que necesitan transporte confiable y que pueden tolerar cierta demora. TCP es un excelente ejemplo de cómo las diferentes capas de la suite de protocolos TCP/IP tienen funciones específicas. Debido a que el protocolo de la capa de transporte TCP maneja todas las tareas asociadas con la segmentación del stream de datos, la confiabilidad, el control del flujo y el reordenamiento de segmentos, este libera a la aplicación de la tarea de administrar cualquiera de estas tareas. La aplicación simplemente puede enviar el stream de datos a la capa de transporte y utilizar los servicios de TCP.

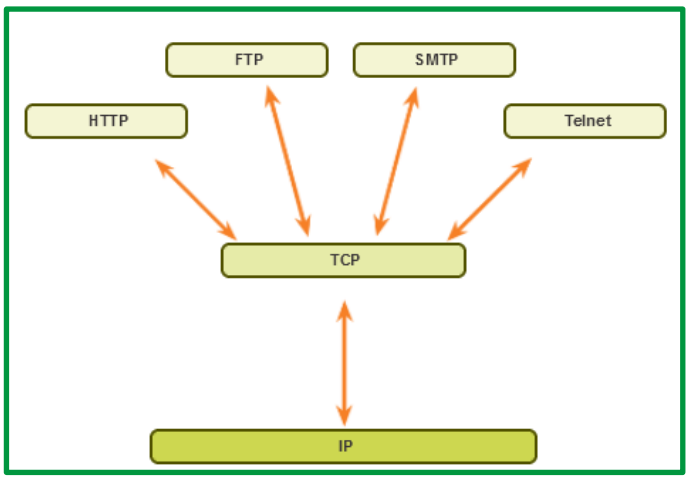


Figure 34. Aplicaciones que Utilizan TCP

Como se muestra en la ilustración, algunos ejemplos de aplicaciones bien conocidas que utilizan TCP incluyen las siguientes:

- Protocolo de transferencia de hipertexto (HTTP)
- Protocolo de transferencia de archivos (FTP)
- Protocolo simple de transferencia de correo (SMTP)
- Telnet

TCP: Aspectos del desempeño

Se dice que TCP está orientado a la conexión porque antes de que un proceso de la capa aplicación pueda comenzar a enviar datos a otro, los dos procesos deben primero "establecer una comunicación" entre ellos; es decir, tienen que enviarse ciertos segmentos preliminares para definir los parámetros de la transferencia de datos que van a llevar a cabo a continuación. Como parte del proceso de establecimiento de la conexión TCP, ambos lados de la misma iniciarán muchas variables de estado TCP asociadas con la conexión TCP.

La "conexión" TCP no es un circuito terminal a terminal con multiplexación TDM o FDM como lo es una red de conmutación de circuitos. En su lugar, la "conexión" es una conexión lógica, con un estado común que reside solo en los niveles TCP de los dos sistemas terminales que se comunican. Dado que el protocolo TCP se ejecuta únicamente en los sistemas terminales y no en los elementos intermedios de la red (routers y switches de la capa de enlace), los elementos intermedios de la red no mantienen el estado de la conexión TCP. De hecho, los routers intermedios son completamente inconscientes de las conexiones TCP; los routers ven los datagramas, no las conexiones.

Una conexión TCP proporciona un servicio full-duplex: si existe una conexión TCP entre el proceso A que se ejecuta en un host y el proceso B que se ejecuta en otro host, entonces los datos de la capa de aplicación pueden fluir desde el proceso A al proceso B en el mismo instante que los datos de la capa de aplicación fluyen del proceso B al proceso A. Una conexión TCP casi siempre es una conexión punto a punto, es decir, entre un único emisor y un único receptor. La "multidifusión", la transferencia de datos desde un emisor a muchos receptores en una única operación de envío, no es posible con TCP. Con TCP, dos hosts son compañía y tres multitudes.

Recuerde que el proceso que inicia la conexión es el proceso cliente, y el otro proceso es el proceso servidor. El proceso de la aplicación cliente informa en primer lugar a la capa de transporte del cliente que desea establecer una conexión con un proceso del servidor. La cantidad máxima de datos que pueden cogerse y colocarse en un segmento está limitada por el tamaño máximo de segmento (MSS, Maximum Segment Size).

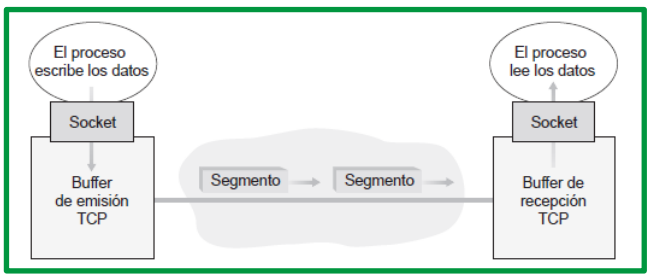


Figure 35. Buffer de emisión y recepción de TCP
Fuente: Libro Redes de computadoras. Un enfoque descendente, 7 Edición

El MSS queda determinado en primer lugar por la longitud de la trama más larga de la capa de enlace que el host emisor local puede enviar [que es la unidad máxima de transmisión, (MTU, Maximum Transmission Unit)], y luego el MSS se establece de manera que se garantice que un segmento TCP (cuando se encapsula en un datagrama IP) más la longitud de la cabecera TCP/IP (normalmente 40 bytes) se ajuste a una única trama de la capa de enlace. Los protocolos de la capa de enlace Ethernet y PPP tienen una MTU de 1.500 bytes. Un valor común de MTU es 1.460 bytes. También se han propuesto métodos para descubrir la MTU de la ruta (la trama más larga de la capa de enlace que puede enviarse a través de todos los enlaces desde el origen hasta el destino) [RFC 1191] y establecer el MSS basándose en el valor de la MTU de la ruta. Observe que el MSS es la cantidad máxima de datos de la capa de aplicación en el segmento, no el tamaño máximo del segmento TCP incluyendo las cabeceras.

TCP empareja cada fragmento de datos del cliente con una cabecera TCP, formando segmentos TCP. Los segmentos se pasan a la capa de red, donde son encapsulados por separado dentro de datagramas IP de la capa de red. Los datagramas IP se envían entonces a la red. Cuando TCP recibe un segmento en el otro extremo, los datos del mismo se colocan en el buffer de recepción de la conexión TCP, como se muestra en la ilustración anterior. La aplicación lee el flujo de datos de este buffer. Cada lado de la conexión tiene su propio buffer de emisión y su propio buffer de recepción.

Por tanto, una conexión TCP consta de buffers, variables y un socket de conexión a un proceso en un host, y otro conjunto de buffers, variables y un socket de conexión a un proceso en otro host. Como hemos mencionado anteriormente, no se asignan ni buffers ni variables a la conexión dentro de los elementos de red (routers, switches y repetidores) existentes entre los hosts.

Suceso	Acción del receptor TCP
Llegada de un segmento en orden con el número de secuencia esperado. Todos los datos hasta el número de secuencia esperado ya han sido reconocidos.	ACK retardado. Esperar hasta durante 500 milisegundos la llegada de otro segmento en orden. Si el siguiente segmento en orden no llega en este intervalo, enviar un ACK.
Llegada de un segmento en orden con el número de secuencia esperado. Hay otro segmento en orden esperando la transmisión de un ACK.	Enviar inmediatamente un único ACK acumulativo, reconociendo ambos segmentos ordenados.
Llegada de un segmento desordenado con un número de secuencia más alto que el esperado. Se detecta un hueco.	Enviar inmediatamente un ACK duplicado, indicando el número de secuencia del siguiente byte esperado (que es el límite inferior del hueco).
Llegada de un segmento que completa parcial o completamente el hueco existente en los datos recibidos.	Enviar inmediatamente un ACK, suponiendo que el segmento comienza en el límite inferior del hueco.

Figure 36. Recomendaciones para la generación de mensajes ACK en TCP [RFC 5681]
Fuente: Libro Redes de computadoras. Un enfoque descendente, 7 Edición

Principios del control de congestión.

Los router realizan retransmisión de paquetes genera congestión de red (la pérdida de un segmento específico de la capa de transporte) pero no se ocupa de la causa de esa congestión (demasiados emisores intentando transmitir datos a una velocidad demasiado alta). Para tratar la causa de la congestión de la red son necesarios mecanismos que regulen el flujo de los emisores en cuanto la congestión de red aparezca.

La congestión de la red se manifiesta en el rendimiento ofrecido a las aplicaciones de la capa superior, pueden aplicarse diversos métodos para evitar la congestión de la red o reaccionar ante la misma. Dentro del presente se establecen tres escenarios:

Escenario 1: dos emisores, un router con buffers de capacidad ilimitada.

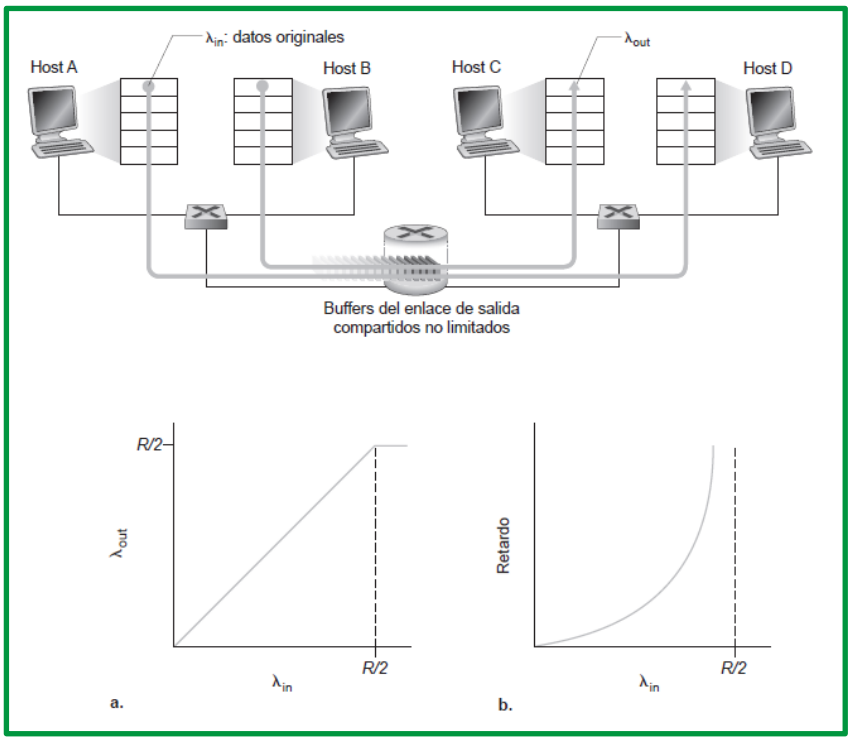


Figure 37. Escenario de congestión 1

La gráfica se muestra la tasa de transferencia por conexión (número de bytes por segundo en el receptor) como una función de la velocidad de transmisión de la conexión. Para una velocidad de transmisión comprendida entre 0 y R/2, la tasa de transferencia en el receptor es igual a la velocidad de transmisión en el emisor (todo lo que envía el emisor es recibido en el receptor con un retardo finito). Sin embargo, cuando la velocidad de transmisión es mayor que R/2, la tasa de transferencia es de solo R/2. Este límite superior de la tasa de transferencia es una consecuencia de compartir entre dos conexiones la capacidad del enlace. El enlace simplemente no puede proporcionar paquetes a un receptor a una velocidad de régimen permanente que sea mayor que R/2. Independientemente de lo altas que sean las velocidades de transmisión de los hosts A y B, nunca verán una tasa de transferencia mayor que R/2.

Escenario 2: dos emisores y un router con buffers finitos

En primer lugar, supongamos que el espacio disponible en los buffers del router es finito. Una consecuencia de esta suposición aplicable en la práctica es que los paquetes serán descartados cuando lleguen a un buffer que ya esté lleno. En segundo lugar, supongamos que cada conexión es fiable. Si un paquete que contiene un segmento de la capa de transporte se descarta en el router, el emisor tendrá que retransmitirlo. Dado que los paquetes pueden retransmitirse, ahora tenemos que ser más cuidadosos al utilizar el término velocidad de transmisión.

El rendimiento de este segundo escenario dependerá en gran medida de cómo se realicen las retransmisiones.

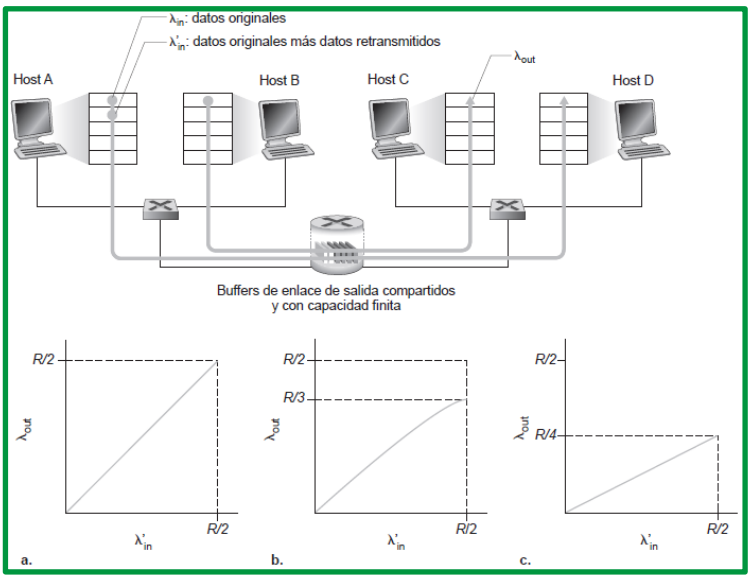


Figure 38. Escenario de congestión 2

Escenario 3: cuatro emisores, routers con buffers de capacidad finita y rutas con múltiples saltos

En este último escenario dedicado a la congestión de red tenemos cuatro hosts que transmiten paquetes a través de rutas solapadas con dos saltos, como se muestra en la ilustración, de nuevo suponemos que cada host utiliza un mecanismo de fin de temporización/retransmisión para implementar un servicio de transferencia de datos fiable, que todos los hosts tienen el mismo valor y que todos los enlaces de router tienen una capacidad de R bytes/segundo.

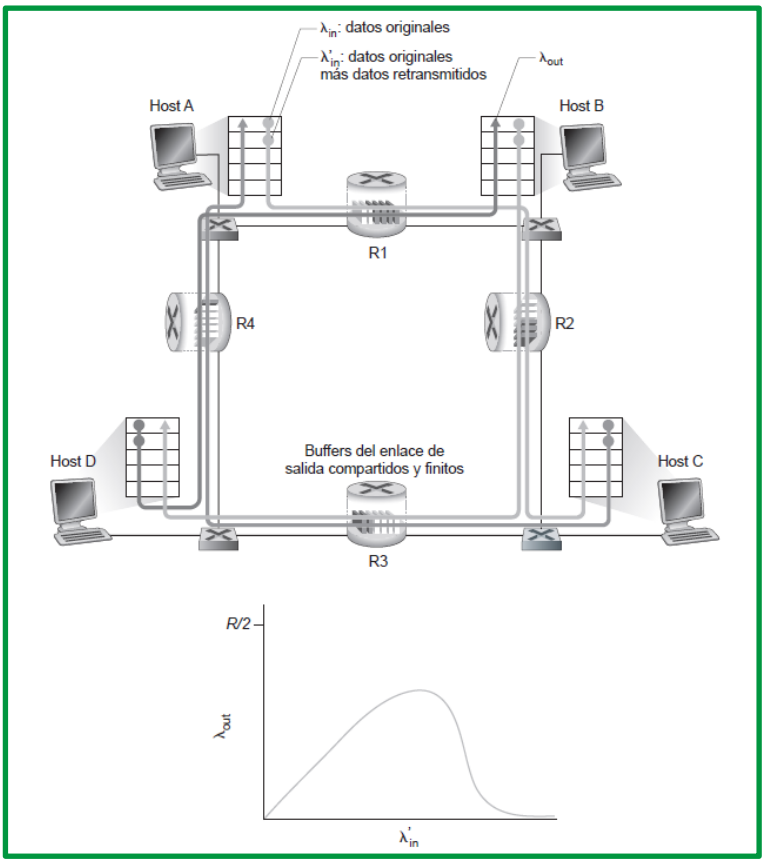


Figure 39. Escenario 3 de congestión

Métodos para controlar la congestión

Los dos métodos más comunes de control de congestión que se utilizan en la práctica:

Control de congestión terminal a terminal. En este método, la capa de red no proporciona soporte explícito a la capa de transporte para propósitos de control de congestión. Incluso la presencia de congestión en la red tiene que ser inferida por los sistemas terminales basándose únicamente en el comportamiento observado de la red (por ejemplo, la pérdida de paquetes y los retardos). TCP tiene que aplicar este método de control de congestión terminal a terminal, ya que la capa IP no proporciona ninguna realimentación a los hosts relativa a la congestión de la red. La pérdida de segmentos TCP (indicada por un fin de temporización o por la recepción de un triple paquete ACK duplicado) se toma como indicación de que existe congestión en la red, por lo que TCP reduce el tamaño de su ventana en consecuencia.

Control de congestión asistido por la red. En este método de control de congestión, los routers proporcionan una realimentación explícita al emisor y/o receptor informando del estado de congestión en la red. Esta realimentación puede ser tan simple como un único bit que indica que existe congestión en un enlace. Este método se aplicó en las tempranas arquitecturas de red SNA de IBM [Schwartz 1982] y DECnet de DEC [Jain 1989; Ramakrishnan 1990] y ATM [Black 1995]. También es posible proporcionar una realimentación de red más sofisticada. Por ejemplo, una forma del mecanismo de control de congestión de ABR (Available Bite Rate) en las redes ATM permite a un router informar al emisor de la velocidad máxima de transmisión de host que el router puede soportar en un enlace saliente. Como conocemos, las versiones predeterminadas

de internet de IP y TCP adoptan un método terminal a terminal para llevar a cabo el control de congestión. Recientemente, IP y TCP pueden implementar de forma opcional un mecanismo de control de congestión asistido por la red.

En el mecanismo de control de congestión asistido por la red, la información acerca de la congestión suele ser realimentada de la red al emisor de una de dos formas; la ***realimentación directa*** puede hacerse desde un router de la red al emisor. Esta forma de notificación, normalmente, toma la forma de un paquete de asfixia o bloqueo (choke packet) (que esencialmente dice "¡Estoy congestionada!"). La segunda forma de notificación, más común, tiene lugar cuando un ***router marca/actualiza un campo*** de un paquete que se transmite del emisor al receptor para indicar que existe congestión. Después de recibir un paquete marcado, el receptor notifica al emisor la existencia de congestión. Es importante conocer que esta última forma de notificación tarda al menos un periodo igual al tiempo de ida y vuelta completo.

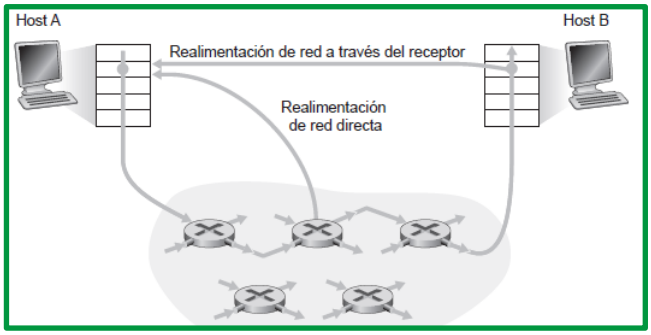


Figure 40. Control de congestión asistido por la red
Fuente: Libro Redes de computadoras. Un enfoque descendente, 7 Edición

El ataque por inundación SYN

En este protocolo de gestión de la conexión TCP establece la base para un ataque DoS clásico, conocido como ataque por inundación SYN. En este ataque, el atacante o atacantes envían un gran número de segmentos SYN TCP, sin completar el tercer paso del proceso de acuerdo. Con esta gran cantidad de segmentos SYN, los recursos de conexión del servidor pueden agotarse rápidamente a medida que se van asignando (¡aunque nunca se utilizan!) a conexiones semiabiertas. Con los recursos del servidor agotados, se niega el servicio a los clientes legítimos. Estos ataques por inundación SYN se encuentran entre los primeros ataques DoS documentados [CERT SYN 1996]. Afortunadamente, existe una defensa efectiva, denominada cookies SYN [RFC 4987], actualmente implantada en la mayoría de los principales sistemas operativos.

Una inundación SYN puede ocurrir de tres maneras diferentes:

Ataque directo: Una inundación SYN en la que la dirección IP no está falsificada se conoce como un "ataque directo". En este ataque, el atacante no oculta su dirección IP. Como el atacante usa un solo dispositivo de origen con una dirección IP real para crear el ataque, el atacante es muy vulnerable a que lo descubran y mitiguen. Para que la máquina que se fija como objetivo quede en estado de semiabierta, el hacker evita que su máquina responda a los paquetes SYN-ACK del servidor. A menudo, esto se logra mediante reglas de firewall que detienen los paquetes salientes que no son SYN, o bien mediante la filtración de paquetes SYN-ACK entrantes antes de que lleguen a la máquina de los usuarios maliciosos.

Ataque de paquetes falsificados: El ataque con una dirección IP falsa es más popular. En este caso, el atacante introduce una dirección IP falsificada en el campo del remitente del paquete SYN y oculta de esta manera su verdadero origen. En este caso, el atacante prefiere utilizar direcciones IP que no estén ocupadas en el momento del ataque. Así se garantiza que los sistemas afectados al azar no reaccionen a las respuestas SYN/ACK del servidor atacado con un paquete RST y terminen así la conexión.

Ataque distribuido (DDoS): Si se genera un ataque mediante una red de bots (botnet), la probabilidad de rastrear el ataque hasta su origen es baja. Para agregar otro nivel de confusión, un atacante puede hacer que cada dispositivo distribuido también falsifique las direcciones IP de las cuales envía los paquetes. Si el atacante usa una red de bots (botnet), por lo general, no se preocupará por ocultar la IP del dispositivo infectado.

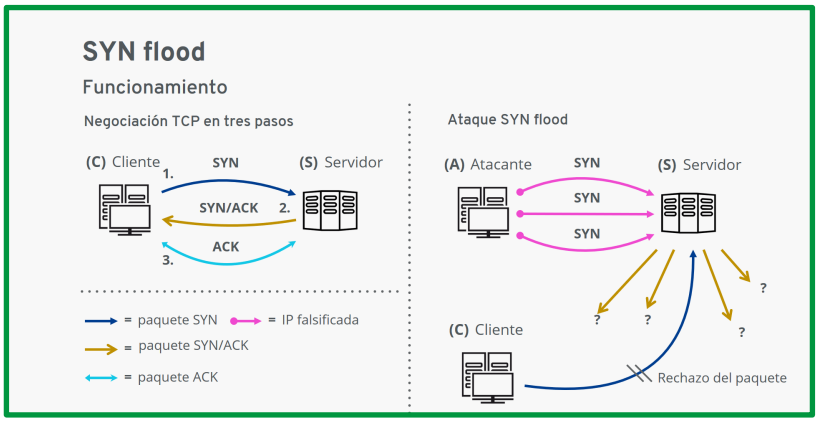


Figure 41. Funcionamiento SYN flood
Fuente: https://www.ionos.es

Protocolos de transporte de internet: UDP.

Si bien las funciones de confiabilidad de TCP proporcionan una comunicación más sólida entre aplicaciones, también representan una sobrecarga adicional y pueden provocar demoras en la transmisión. Existe una compensación entre el valor de la confiabilidad y la carga que implica para los recursos de la red. La imposición de sobrecarga para garantizar la confiabilidad para algunas aplicaciones podría reducir la utilidad a la aplicación e incluso ser perjudicial para esta. En estos casos, UDP es un protocolo de transporte mejor.

UDP proporciona solo las funciones básicas para entregar segmentos de datos entre las aplicaciones adecuadas, con muy poca sobrecarga y revisión de datos. El protocolo UDP se conoce como protocolo de entrega de máximo esfuerzo. En el contexto de redes, la entrega de máximo esfuerzo se denomina “poco confiable”, porque no hay acuse de recibo que indique que los datos se recibieron en el destino. Con UDP, no existen procesos de capa de transporte que informen al emisor si la entrega se produjo correctamente.

El proceso de UDP es similar al envío por correo de una carta simple sin registrar. El emisor de la carta no sabe si el receptor está disponible para recibir la carta ni la oficina de correos es responsable de hacer un seguimiento de la carta o de informar al emisor si esta no llega a destino.

UDP se considera un protocolo de transporte de máximo esfuerzo, descrito en RFC 768. UDP es un protocolo de transporte liviano que ofrece la misma segmentación y rearmado de datos que

TCP, pero sin la confiabilidad y el control del flujo de TCP. UDP es un protocolo tan simple que, por lo general, se lo describe en términos de lo que no hace en comparación con TCP.

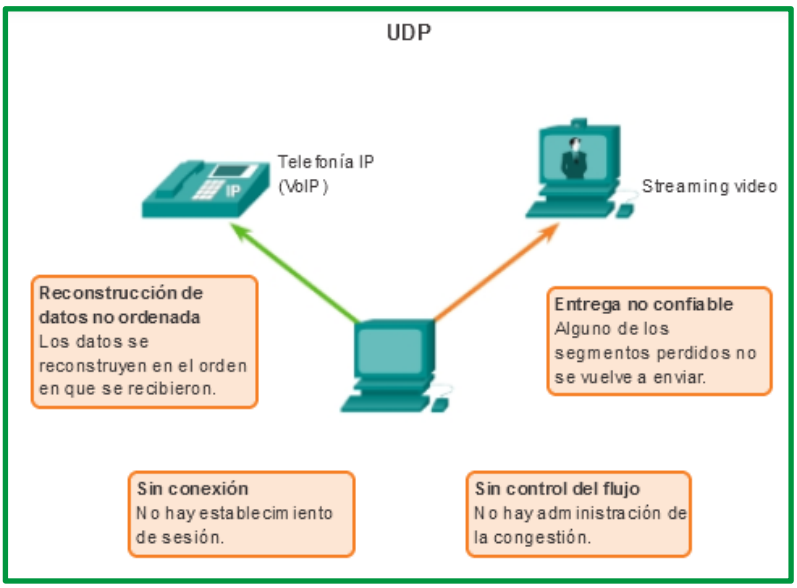


Figure 42. Protocolo UDP

Las siguientes características describen a UDP:

- ***Sin conexión***: UDP no establece una conexión entre los hosts antes de que se puedan enviar y recibir datos.
- ***Entrega no confiable***: UDP no proporciona servicios para asegurar que los datos se entreguen con confianza. UDP no cuenta con procesos que hagan que el emisor vuelva a transmitir los datos que se pierden o se dañan.
- ***Reconstrucción de datos no ordenada***: en ocasiones, los datos se reciben en un orden distinto del de envío. UDP no proporciona ningún mecanismo para rearmar los datos en su secuencia original. Los datos simplemente se entregan a la aplicación en el orden en que llegan.
- ***Sin control del flujo***: UDP no cuenta con mecanismos para controlar la cantidad de datos que transmite el dispositivo de origen para evitar la saturación del dispositivo de destino. El origen envía los datos. Si los recursos en el host de destino se sobrecargan, es probable que dicho host descarte los datos enviados hasta que los recursos estén disponibles. A diferencia de TCP, en UDP no hay un mecanismo para la retransmisión automática de datos descartados.

Aunque UDP no incluye la confiabilidad y los mecanismos de control del flujo de TCP, la entrega de datos de baja sobrecarga de UDP lo convierte en un protocolo de transporte ideal para las aplicaciones que pueden tolerar cierta pérdida de datos. Las porciones de comunicación en UDP se llaman datagramas. El protocolo de la capa de transporte envía estos datagramas como máximo esfuerzo. Algunas aplicaciones que utilizan UDP son el Sistema de nombres de dominios (DNS), el streaming de video y la voz sobre IP (VoIP).

Uno de los requisitos más importantes para transmitir video en vivo y voz a través de la red es que los datos fluyan rápidamente. Las aplicaciones de video y de voz pueden tolerar cierta

pérdida de datos con un efecto mínimo o imperceptible, y se adaptan perfectamente a UDP. A continuación, se detallan algunas aplicaciones que utilizan UDP.

Número de puerto	Aplicación
53	DNS
67	DHCP Servidor
68	DHCP Cliente
69	TFTP
161	SNMP
514	Syslog

Tabla 2. Aplicaciones que utilizan protocolos UDP

Existen tres tipos de aplicaciones que son las más adecuadas para UDP:

- Aplicaciones que pueden tolerar cierta pérdida de datos, pero requieren retrasos cortos o que no haya retrasos
- Aplicaciones con transacciones de solicitud y respuesta simples
- Comunicaciones unidireccionales donde no se requiere confiabilidad o donde la aplicación la pueda administrar

Muchas aplicaciones de video y multimedia, como VoIP y la televisión por protocolo de Internet (IPTV), utilizan UDP. Estas aplicaciones pueden tolerar cierta pérdida de datos con un efecto mínimo o imperceptible. Los mecanismos de confiabilidad de TCP presentan cierto grado de demora que se puede percibir en la calidad de sonido o video que se recibe.

Otros tipos de aplicaciones adecuadas para UDP son las que utilizan transacciones de solicitud y respuesta simples. Esto se da cuando un host envía una solicitud y existe la posibilidad de que reciba una respuesta o no. Estos tipos de aplicaciones incluyen las siguientes:

- DHCP
- DNS: también puede utilizar TCP
- SNMP
- TFTP

Algunas aplicaciones se ocupan de la confiabilidad por sí mismas. Estas aplicaciones no necesitan los servicios de TCP y pueden utilizar mejor UDP como protocolo de capa de transporte. TFTP es un ejemplo de este tipo de protocolo. TFTP tiene sus propios mecanismos para el control del flujo, la detección de errores, los acuses de recibo y la recuperación de errores. Este protocolo no necesita depender de TCP para esos servicios.

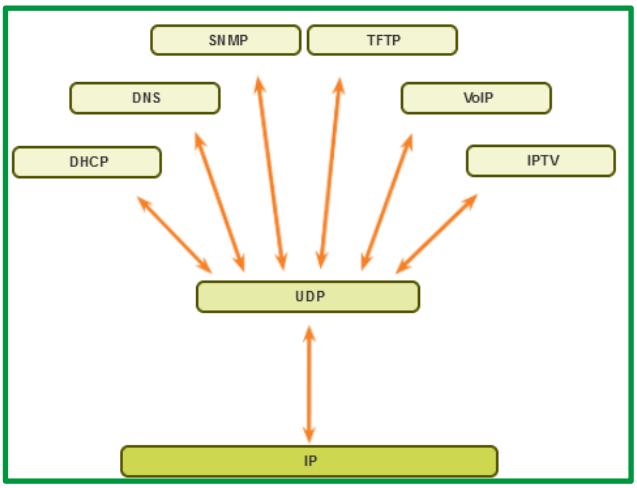


Figure 43. Aplicaciones que utiliza UDP

Fragmentación, Multiplexación, Aspectos del desempeño

UDP es un protocolo sin estado, lo cual significa que ni el cliente ni el servidor están obligados a hacer un seguimiento del estado de la sesión de comunicación. Como se muestra en la ilustración, UDP no se ocupa de la confiabilidad ni del control del flujo. Los datos se pueden perder o recibir fuera de secuencia sin ningún mecanismo de UDP que pueda recuperarlos o reordenarlos. Si se requiere confiabilidad al utilizar UDP como protocolo de transporte, está la debe administrar la aplicación.

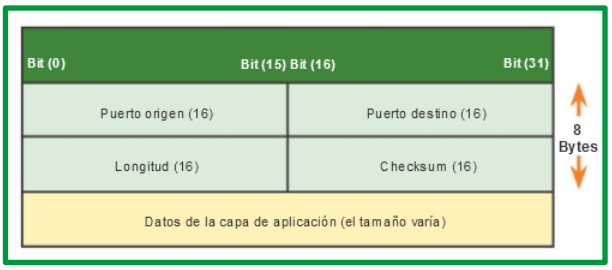


Figure 44. Datagrama UDP

La diferencia clave entre TCP y UDP es la confiabilidad. La confiabilidad de la comunicación TCP se obtiene con el uso de sesiones orientadas a la conexión. Antes de que un host que utiliza TCP envíe datos a otro host, TCP inicia un proceso para crear una conexión con el destino. Esta conexión con estado permite hacer un seguimiento de una sesión o un stream de comunicación entre los hosts. Este proceso asegura que cada host tenga conocimiento del stream de comunicación y se prepare para este. Una conversación TCP requiere que se establezca una sesión entre hosts en ambas direcciones. Una vez que se establece una sesión y que comienza la transferencia de datos, el destino envía acuses de recibo al origen por los segmentos que recibe. Estos acuses de recibo forman la base de la confiabilidad dentro de la sesión TCP. Cuando el origen recibe un acuse de recibo, reconoce que los datos se entregaron correctamente y puede dejar de rastrearlos. Si el origen no recibe el acuse de recibo dentro de un tiempo predeterminado, retransmite esos datos al destino.

UDP es un protocolo simple que proporciona las funciones básicas de la capa de transporte. Tiene una sobrecarga mucho menor que TCP, ya que no está orientado a la conexión y no

proporciona los mecanismos sofisticados de retransmisión, secuenciación y control del flujo que ofrecen confiabilidad.

Esto no significa que las aplicaciones que utiliza UDP sean siempre poco confiables ni que UDP sea un protocolo inferior. Solo quiere decir que estas funciones no las proporciona el protocolo de la capa de transporte, y se deben implementar aparte, si fuera necesario.

Pese a que es relativamente baja la cantidad total de tráfico UDP que puede encontrarse en una red típica, los protocolos clave de la capa de aplicación que utilizan UDP incluyen lo siguiente:

- Sistema de nombres de dominio (DNS)
- Protocolo simple de administración de red (SNMP, Simple Network Management Protocol)
- Protocolo de configuración dinámica de host (DHCP)
- Protocolo de información de enrutamiento (RIP)
- Protocolo de transferencia de archivos trivial (TFTP)
- Telefonía IP o voz sobre IP (VoIP)
- Juegos en línea

Figure 45. Transporte de Datos UDP

Algunas aplicaciones, como los juegos en línea o VoIP, pueden tolerar cierta pérdida de datos. Si estas aplicaciones utilizaran TCP, experimentarían largas demoras, ya que TCP detecta la pérdida de datos y los retransmite. Estas demoras serían más perjudiciales para el rendimiento de la aplicación que las pequeñas pérdidas de datos. Algunas aplicaciones, como DNS, simplemente reintentan el envío de la solicitud si no reciben ninguna respuesta; por lo tanto, no necesitan que TCP garantice la entrega de mensajes. La baja sobrecarga del UDP es deseada por dichas aplicaciones.

Ya que UDP opera sin conexión, las sesiones no se establecen antes de que se lleve a cabo la comunicación, como sucede con TCP. Se dice que UDP está basado en las transacciones; es decir, cuando una aplicación tiene datos para enviar, simplemente los envía.

Muchas aplicaciones que utilizan UDP envían pequeñas cantidades de datos que pueden ajustarse en un segmento. Sin embargo, algunas aplicaciones envían cantidades de datos más grandes que deben dividirse en varios segmentos. La PDU del UDP se conoce como un "***datagrama***", aunque los términos "***segmento***" y "***datagrama***" se utilizan algunas veces de forma intercambiable para describir una PDU de la capa de transporte.

Cuando se envían datagramas múltiples a un destino, pueden tomar diferentes rutas y llegar en el orden equivocado. UDP no realiza un seguimiento de los números de secuencia de la manera en que lo hace TCP. UDP no tiene forma de reordenar datagramas en el orden en que se transmiten, como se muestra en la ilustración.

Por lo tanto, UDP simplemente reensambla los datos en el orden en que se recibieron y los envía a la aplicación. Si la secuencia de datos es importante para la aplicación, esta debe identificar la secuencia adecuada y determinar cómo se deben procesar los datos.

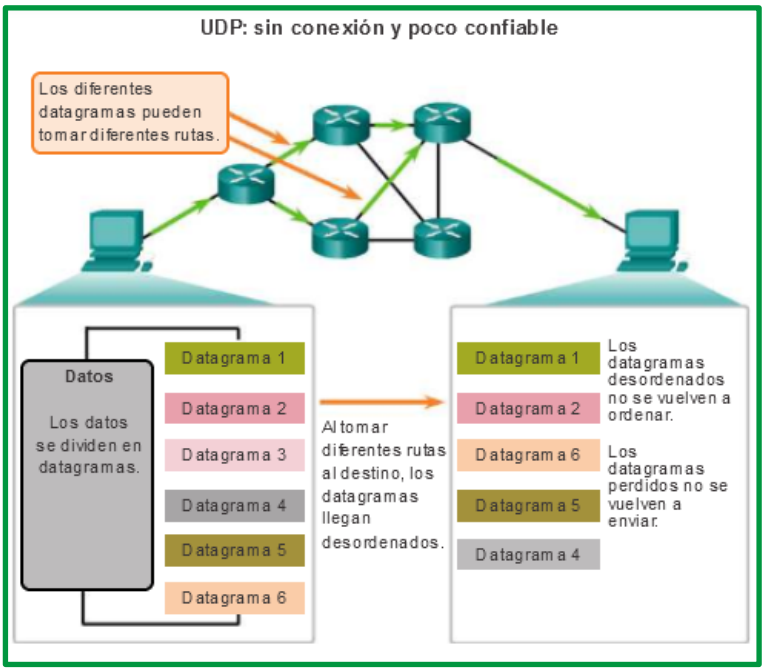


Figure 46. Datagramas UDP

Al igual que las aplicaciones basadas en TCP, a las aplicaciones de servidor basadas en UDP se les asignan números de puerto bien conocidos o registrados. Cuando estas aplicaciones o estos procesos se ejecutan en un servidor, aceptan los datos que coinciden con el número de puerto asignado. Cuando UDP recibe un datagrama destinado a uno de esos puertos, envía los datos de aplicación a la aplicación adecuada en base a su número de puerto.

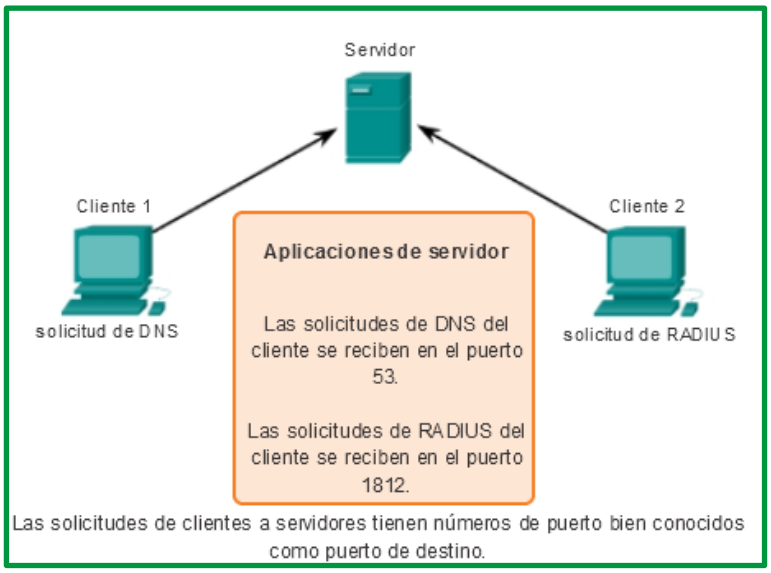


Figure 47. Servidor UDP a la escucha de solicitudes

Como en TCP, la comunicación cliente/servidor la inicia una aplicación cliente que solicita datos de un proceso de servidor. El proceso de cliente UDP selecciona al azar un número de puerto del rango de números de puerto dinámicos y lo utiliza como puerto de origen para la conversación. Por lo general, el puerto de destino es el número de puerto bien conocido o registrado que se asigna al proceso de servidor.

Los números de puerto de origen seleccionados al azar colaboran con la seguridad. Si existe un patrón predecible para la selección del puerto de destino, un intruso puede simular el acceso a un cliente de manera más sencilla intentando conectarse al número de puerto que tenga mayor posibilidad de estar abierto.

Dado que no se crean sesiones con UDP, no bien los datos están listos para enviarse y los puertos están identificados, UDP puede formar los datagramas y pasarlos a la capa de red para direccionarlos y enviarlos a la red.

Una vez que el cliente selecciona los puertos de origen y de destino, este mismo par de puertos se utiliza en el encabezado de todos los datagramas que se utilizan en la transacción. Para la devolución de datos del servidor al cliente, se invierten los números de puerto de origen y destino en el encabezado del datagrama.

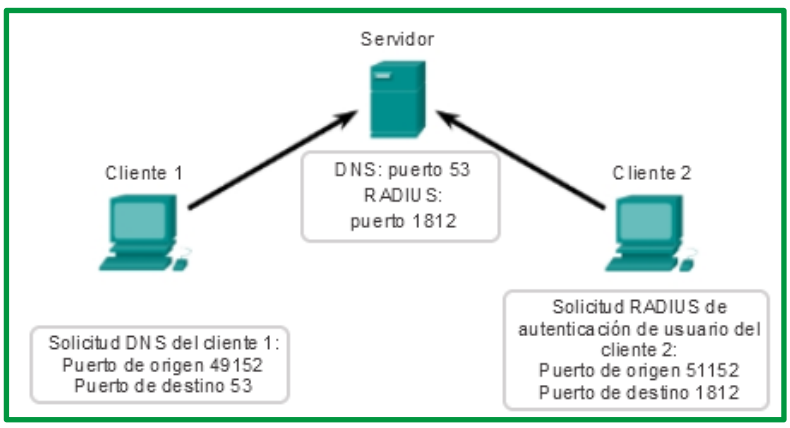


Figure 48.Ejemplo de procesos de cliente UDP

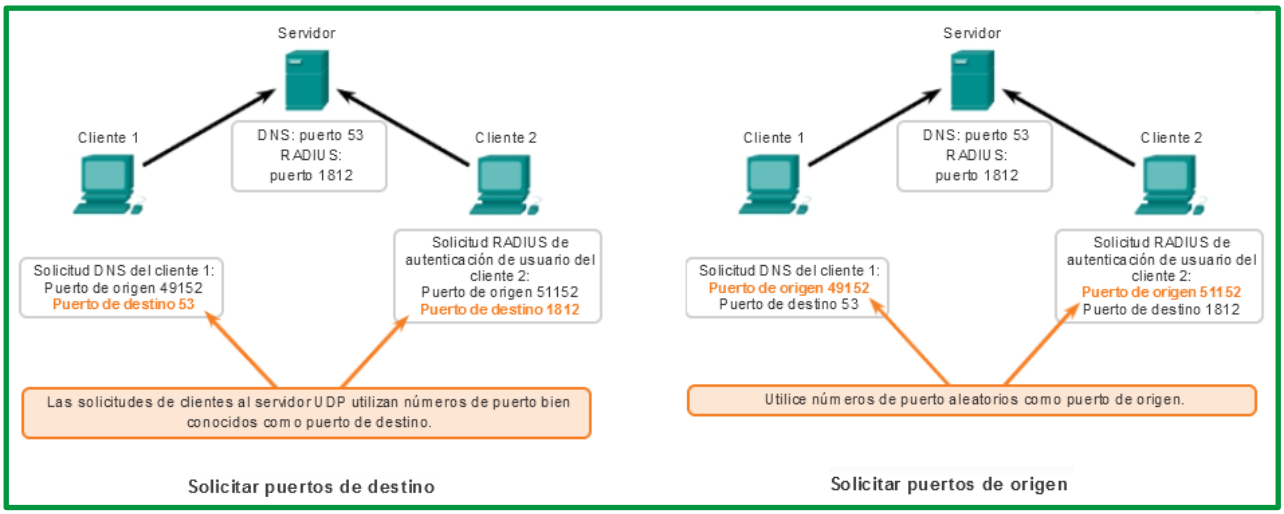


Figure 49. Proceso de solicitud de puertos UDP

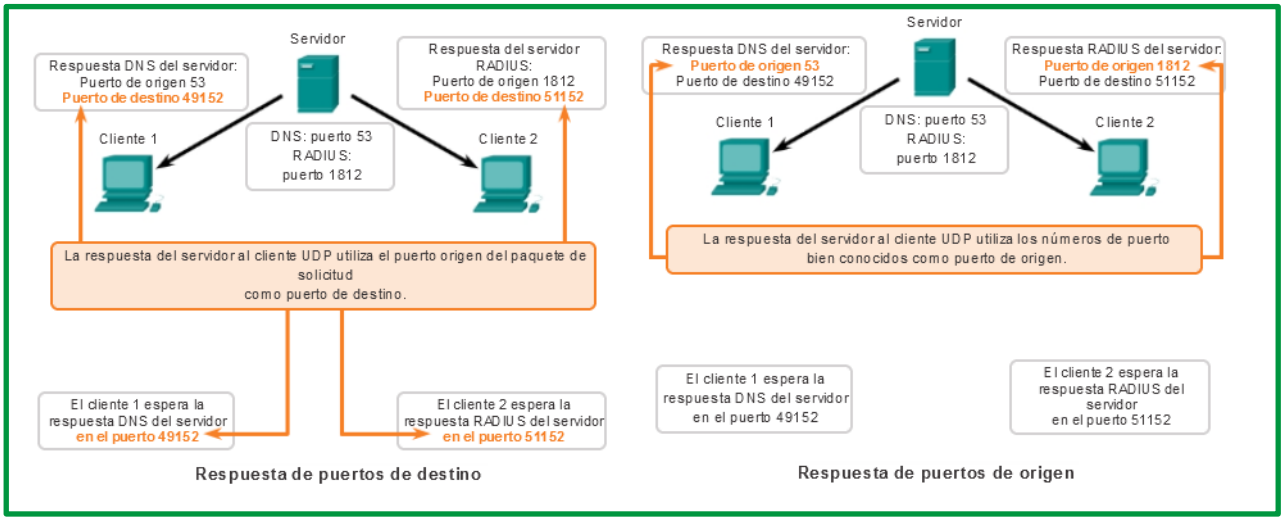


Figure 50. Proceso de respuesta de puertos UDP

Suma de comprobación de UDP

La suma de comprobación de UDP proporciona un mecanismo de detección de errores. Es decir, se utiliza para determinar si los bits contenidos en el segmento UDP han sido alterados según se desplazaban desde el origen hasta el destino (por ejemplo, a causa de la existencia de ruido en los enlaces o mientras estaban almacenados en un router). UDP en el lado del emisor calcula el complemento a 1 de la suma de todas las palabras de 16 bits del segmento, acarreando cualquier desbordamiento obtenido durante la operación de suma sobre el bit de menor peso. Este resultado se almacena en el campo suma de comprobación del segmento UDP. He aquí un ejemplo sencillo de cálculo de una suma de comprobación. Puede obtener información detallada acerca de una implementación eficiente del cálculo en el RFC 1071, así como de su rendimiento con datos reales en [Stone 1998; Stone 2000]. Por ejemplo, suponga que tenemos las siguientes tres palabras de 16 bits:

0110011001100000
0101010101010101
1000111100001100

La suma de las dos primeras palabras de 16 bits es:

0110011001100000
0101010101010101

1011101110110101

Sumando la tercera palabra a la suma anterior, obtenemos,

1011101110110101
1000111100001100

0100101011000010

Observe que en esta última suma se produce un desbordamiento, el cual se acarrea sobre el bit de menor peso. El complemento a 1 se obtiene convirtiendo todos los 0 en 1 y todos los 1 en 0. Por tanto, el complemento a 1 de la suma 0100101011000010 es 1011010100111101, que es la suma de comprobación. En el receptor, las cuatro palabras de 16 bits se suman, incluyendo la suma de comprobación. Si no se han introducido errores en el paquete, entonces la suma en el receptor tiene que ser 1111111111111111. Si uno de los bits es un 0, entonces sabemos que el paquete contiene errores.
Dado que IP está pensado para ejecutarse sobre prácticamente cualquier protocolo de la capa 2, resulta útil para la capa de transporte proporcionar un mecanismo de comprobación de errores como medida de seguridad. Aunque UDP proporciona un mecanismo de comprobación de errores, no hace nada para recuperarse del error. Algunas implementaciones de UDP simplemente descartan el segmento dañado y otras lo pasan a la aplicación junto con una advertencia.

Finalmente se puede señalar que UDP necesita menos bytes en la cabecera por lo que utiliza menos ancho de banda y necesita menos consumo procesamiento.

Figure 51. Comparación de características de TCP y UDP

La capa de transporte proporciona servicios relacionados con el transporte de las siguientes maneras:

- La división en segmentos de los datos que se reciben de una aplicación
- La adición de un encabezado para identificar y administrar cada segmento
- El uso de la información del encabezado para reensamblar los segmentos de nuevo en datos de aplicación
- El paso de los datos ensamblados hacia la aplicación correcta

UDP y TCP son protocolos de la capa de transporte comunes.

Los datagramas de UDP y los segmentos TCP tienen encabezados que se agregan delante de los datos, los cuales incluyen un número de puerto de origen y un número de puerto de destino. Estos números de puerto permiten que los datos se dirijan a la aplicación correcta que se ejecuta en la computadora de destino.

El TCP pasa datos a la red hasta que conoce el destino y está listo para recibirlo. Luego TCP administra el flujo de datos y reenvía todos los segmentos de datos de los que recibió acuse a medida que se reciben en el destino. TCP utiliza mecanismos de enlace, temporizadores, mensajes de acuse de recibo y control del flujo mediante mecanismo ventana dinámico para lograr la confiabilidad. El proceso de confiabilidad, sin embargo, impone una sobrecarga en la red en términos de encabezados de segmentos mucho más grandes y más tráfico de la red entre el origen y el destino.

Si se deben entregar los datos de aplicación a través de la red de manera rápida, o si el ancho de banda de la red no admite la sobrecarga de mensajes de control que se intercambian entre los sistemas de origen y destino, UDP es el protocolo de la capa de transporte preferido por los desarrolladores. Esto es así porque UDP no rastrea ni acusa recibo de datagramas en el destino (solo envía los datagramas recibidos a la capa de aplicación a medida que llegan) ni reenvía datagramas perdidos. Sin embargo, esto no significa necesariamente que la comunicación misma no sea confiable; puede haber mecanismos en los protocolos de la capa de aplicación y servicios que procesen datagramas perdidos o retrasados si la aplicación tiene estos requisitos.

El desarrollador de la aplicación decide cuál es el protocolo de capa de transporte que más se ajusta a los requisitos de la aplicación. Es importante recordar que el resto de las capas cumplen una función en las comunicaciones de red de datos y afectan el rendimiento de estas.

Lectura complementaria de la asignatura

Dentro de los materiales y herramientas de la unidad 4 se encuentran el libro de "Redes de computadoras. Un enfoque descendente, 7 Edición" de autoría de James F. Kurose y Keith W. Ross.

Sitio web de cual se recuperó el contenido del libro en su séptima edición es : https://www.academia.edu/40738627/Redes_de_computadoras_Un_enfoque_descendente_7a_Edici%C3%B3n. Estará publicado en plataforma como recursos complementarios donde podrá revisar el capítulo 3 referente a la capa de transporte.

Bibliografía

Universidad de Salamanca. (27 de 06 de 2011). Recuperado el 20 de 06 de 2021, de http://campus.usal.es/

Área de Ingeniería Telemática. (s.f.). *Universidad Pública de Navarra*. Recuperado el 19 de 06 de 2021, de http://www.tlm.unavarra.es

Calvo, R. A. (s.f.). *Universidad de Cantabria*. Recuperado el 19 de 06 de 2021, de Grupo de Ingeniería Telemática (GIT): https://www.tlmat.unican.es/

ccnadesdecero.com. (s.f.). *CCNA Desde Cero.* Recuperado el 26 de 05 de 2021, de https://ccnadesdecero.com/curso/tipos-de-direcciones-ipv6/

Cisco Networking Academy ITESA. (s.f.). *nstituto Tecnológico Superior del Oriente del Estado de Hidalgo*. Recuperado el 27 de 06 de 2021, de https://www.itesa.edu.mx/netacad/

Class Virtual. (s.f.). Recuperado el 26 de 05 de 2021, de https://eclassvirtual.com/tipos-de-direcciones-ipv6-cisco-ccna/

Deep Medhi, K. R. (s.f.). Recuperado el 19 de 06 de 2021

Fernando Boronat Seguí, M. M. (2013). *Direccionamiento e Interconexión de redes basadas en TCP/IP* (Primera edición, 2013 ed.). Universidad Politécnica de Válencia. Recuperado el 20 de 06 de 2021, de www.editorial.upv.es

Ginno Millán, G. F. (17 de 10 de 2018). A Simple and Fast Algorithm for Traffic Flow . 4. doi:10.1109/ICA-ACCA.2018.8609857

Goitia, M. J. (s.f.). *UNIVERSIDAD NACIONAL DEL NORDESTE*. Recuperado el 19 de 06 de 2021, de http://exa.unne.edu.ar/informatica/SO/ProtocolosRed.PDF

Gutiérrez, A. E. (s.f.). *OpenCourseWare* . Recuperado el 20 de 06 de 2021, de https://ocw.unican.es/pluginfile.php/1357/course/section/1682/Tema%202.pdf

Hernández, M. Á. (09 de 2009). *Universidad de Valladolid*. Recuperado el 12 de 06 de 2021, de Escuela Técnica Su perior de telecomunicación: http://www.tel.uva.es

Leiva, Y. E. (09 de 2014). *http://www.inf.udec.cl*. Recuperado el 12 de 06 de 2021, de http://www.inf.udec.cl

Pedraza, L. F. (11 de 12 de 20211). Enrutamiento basado en el algoritmo de Dijkstra para una red de radio cognitiva. *15*(30). doi:ISSN 0123-921X

Unidersidad de Valencia. (s.f.). *Departamento de Informatica*. Recuperado el 26 de 05 de 2021, de http://informatica.uv.es/iiguia/AER/Tema6_IPX.pdf

Universidad de Oviedo. (05 de 03 de 2012). *Departamento de Ingeniería Eléctrica, Electrónica, de Computadores y de Sistemas*. Recuperado el 12 de 06 de 2021, de http://www.isa.uniovi.es/docencia/redes/

Alejandro Fabian Mero García, Ingeniero en sistemas informáticos de profesión, nació en la ciudad de Portoviejo el 17 de julio de 1985, hijo primogénito de Segundo Mero y Mercedes García. Cursó sus estudios primarios en la escuela fiscal Mixta Gregorio Pita Andrade, su educación básica superior en el Colegio Técnico Santa Ana y el bachillerato en la Unidad Educativa Informática Portoviejo, sus estudios de tercer nivel en la Universidad Técnica de Manabí (UTM), especializándose como Magister en Redes de computación en la PUCE. En su trayectoria laboral resaltan instituciones como: PUNTONET S.A., Dirección Distrital 13D04 de Salud, Universidad Técnica de Manabí; desempeñándose en la actualidad como responsable de la unidad de Tics del Hospital de Especialidades de Portoviejo, a demás de docente de tiempo parcial en la UTM.

Cesar Armando Moreira Zambrano, Ingeniero en sistemas informáticos de profesión por la Universidad Técnica de Manabí (UTM), Master en Redes de comunicación por la Pontificia Universidad Católica del Ecuador PUCE. En su trayectoria laboral resaltan instituciones como: la ESPAM MFL, Creador del programa de maestría en ciberseguridad, docente de posgrado Municipio de Tosagua, Docente de la Universidad Técnica de Manabí. Define línea de investigación ciberseguridad y Ciberdefensa, cómputo forense, redes de comunicación, administración de servidores. Cloud computing.

Walter Zambrano Romero, Ingeniero en sistemas informáticos de profesión por la Universidad Técnica de Manabí (UTM), Master en Redes de comunicación por la Pontificia Universidad Católica del Ecuador PUCE. En su trayectoria laboral resaltan instituciones como: la Hospital Miguel H Alcívar, Creador del programa de tercer nivel coordinador de maestría en software, docente de posgrado, Docente de la Universidad Técnica de Manabí. Define línea de investigación Tecnologías disruptivas, cloud Computing, redes de comunicación.

Dannyll Michellc Zambrano Zambrano, Ingeniero en electrónica y redes, Master en Redes de comunicación por la Pontificia Universidad Católica del Ecuador PUCE. En su trayectoria laboral resaltan instituciones como: la Contraloría General del Estado, Decano de la Facultad de Ciencias Informáticas, docente de posgrado, Docente de la Universidad Técnica de Manabí. Define línea de investigación Tecnologías de la información y comunicación, redes de comunicación.

Duglas Antonio Mendoza Briones, Licenciado en Informática graduado en la Universidad Laica Eloy Alfaro de Manabí, Master en Redes de Comunicación por la Pontificia Universidad Católica del Ecuador PUCE. En su trayectoria laboral resaltan instituciones como: Docente de la Universidad Técnica de Manabí, Docente de la PUCE campus Chone, Docente de la ULEAM Extensión Chone, Administrador TIC en Hospital Básico San Andres. Experto en desarrollo de software, bases de datos y cámaras de seguridad y redes de comunicación.

Leonardo Chancay García Ingeniero en Sistemas Informáticos por la UTM, Máster en Ingeniería de Computadoras y Redes y Doctor en Informática por parte de la Universidad Politècnica de Valencia donde trabajo como investigador en el Grupo de Redes de Computadora, y ha trabajo en varios proyectos de redes, con protocolos de enrutamiento en redes Manets y Vanets, redes oportunistas y redes tolerantes a retardo. Actualmente en la Universidad Tecnica de Manabi está trabajando en varios proyectos de IoT e ITS.
Mail: leonardo.chancay@utm.edu.ec

Camilo Jacinto Coronel Escobar, actualmente Docente Universidad de Guayaquil, Facultad de Ciencias Psicológicas del área de conocimiento Tecnología, Magister En Educación Informática, Licenciado en Ciencias de la Educación con Especialización en Informática, Profesor de Segunda Enseñanza en Informática, Tecnólogo Pedagógico en Informática, Docente del Instituto Tecnológico Guayaquil, docente a nivel medio Unidad Educativa Bernardino Echeverría, imparte las asignaturas del área técnica. camilo.coronele@ug.edu.ec

Jaime Gabriel Espinosa Izquierdo, Tecnólogo Pedagógico en Informática, Profesor de Segunda Enseñanza en Informática. Licenciado en Ciencias de la Educación con Especialización en Informática, Magister En Educación Informática, docente a nivel medio, actualmente docente de la Universidad de Guayaquil, Facultad de Filosofía Letras y Ciencias de la Educación, Carrera Pedagogía de las Ciencias Experimentales-Informática. Tutor Académico de pregrado de la Universidad de Guayaquil. Revisor Académico de la Facultad de Filosofía, Letras y Ciencias de la Educación. Participación en Eventos Científicos a nivel Nacional e Internacional. Publicación de Artículos Científicos en revistas arbitradas. Autor de libros de Tecnología registrados en el IEPI y Cámara de Libros. Condecoración al Mérito Educativo. Cuenta con su Identidad digital.

ISBN: 978-9942-33-598-2

@grupocompas.ec
compasacademico@icloud.com