UNIVERSIDAD AUTÓNOMA METROPOLITANA
AZCAPOTZALCO

División de Ciencias Básicas e Ingeniería

DISEÑO E IMPLANTACIÓN DE UNA LAN VIRTUAL CON SWITCHES DE RED

PROYECTO TERMINAL QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

PRESENTA

JUAN ALBERTO CASTILLO CABRERA

MATRÍCULA

204242208

ASESOR

MTRO. JOSÉ IGNACIO VEGA LUNA

JULIO 2010

A la Profesora María Guadalupe Elba Cabrera Trejo

MI MADRE

Índice de contenido

1. Introducción

Los seres humanos como entes sociales, tenemos inherentemente la necesidad de comunicarnos entre nosotros. Desde los primeros signos de vida de la humanidad, la *comunicación* ha jugado un papel preponderante en su lucha por la supervivencia y para la satisfacción de necesidades básicas. Cuando éstas han sido cubiertas, surgen nuevas necesidades paralelamente al ritmo del desarrollo humano de cada época, pues si bien la alimentación, el vestido y la supervivencia fueron esenciales en un principio, la aspiración del hombre a un nivel de vida con mayores comodidades ha traído como consecuencia la búsqueda de técnicas y herramientas cada vez más sofisticadas.

Es a partir de este momento cuando se inicia el desarrollo tecnológico de la humanidad, llegando hasta el siglo XX, considerado el siglo de mayor avance científico, tecnológico e industrial del hombre. Las comunicaciones como el teléfono, la radio, la televisión y el transporte contribuyeron de forma importante a este avance, sin embargo, la llegada de las tecnologías de la información ha marcado un hito histórico en el consecuente desarrollo de las sociedades. Pues si bien la televisión y la radio satisficieron ciertas necesidades de información, no fueron suficientes, al no permitir la interacción bidireccional así como la retroalimentación.

Con la creación de la computadora, se marcó una nueva etapa científico-tecnológica del hombre, permitiéndole el procesamiento de información con mayor rapidez y eficiencia. Los equipos de investigación de las grandes universidades y organismos gubernamentales se avocaron a desarrollar el potencial impacto de la estrecha relación entre la tecnología, la comunicación y las computadoras, a través de la sistematización de la información por medio de la creación de dispositivos tecnológicos y lenguajes especializados capaces de facilitar el procesamiento, el manejo, el almacenamiento y la difusión de datos. Esta sistematización permitió un aprovechamiento más eficiente de los recursos informáticos para ponerlos al alcance de la sociedad en general.

Estas tecnologías de la información se desarrollaron tan rápidamente debido en parte a las guerras o a la amenaza de ellas (Guerra Fría), pues hubo aplicaciones

computacionales asociadas a la investigación y el desarrollo bélico. La radio, el radar y la grabación de sonidos fueron tecnologías clave que allanaron el camino del almacenamiento magnético de datos.

En un principio se inventaron dispositivos de almacenamiento para diferentes tipos de información, como el ahora obsoleto *disquete* y las cintas magnéticas que en la actualidad se siguen ocupando en algunos casos. Sin embargo, no fueron suficientes para la magnitud de las necesidades de almacenamiento e intercambio de información, lo cual llevó a la invención de técnicas para conectar estas máquinas computadoras entre sí por medio de cables para compartir toda clase de datos sin utilizar dispositivos de almacenamiento externos, con el objeto de reducir tiempos, acortar distancias y facilitar el intercambio, creando lo que con el tiempo se conocería como **redes de computadoras**.

Pues si bien las redes se crearon antes del *disquete,* estas sólo fueron utilizadas por algunas instituciones para diversos proyectos internos, como el Departamento de Defensa de los Estados Unidos, la Universidad de Berkeley y el Instituto Tecnológico de Massachusetts, entre otras. Esto evidenció la necesidad de expandir esta forma de intercambio de información a todo el mundo debido a la rapidez y eficiencia en la comunicación, generando que en la década de los 80' surgieran las primeras bases de lo que ahora se conoce como **Internet**.

Este tipo de infraestructuras de red empezó a propagarse por el planeta, atravesó países occidentales e inició una penetración en los países en desarrollo, creando un acceso mundial a la información y a la comunicación sin precedentes, creando también una relativa **brecha digital** en el acceso a esta nueva tecnología. Las redes también modificaron la economía global y la forma en que operaban los negocios. Con la introducción de la **World Wide Web** y las **.com** era evidente que la forma en la que el mundo se desarrollaría en los años futuros cambiaría extraordinariamente.

En la actualidad nos encontramos en un momento decisivo respecto del uso de la tecnología para extender y potenciar nuestra **red humana**. La globalización ha traído nuevas formas de comunicación como la antes mencionada Internet que ha evolucionado más rápido de lo que cualquiera hubiera imaginado. El modo en el que

se producen las interacciones sociales, comerciales, políticas y personales cambia en forma continua para estar al día con la evolución de esta red global. Esto ha permitido la implementación de esta herramienta como auxiliar en diversas áreas del desarrollo humano, como la ciencia, la educación, el comercio y por supuesto las relaciones interpersonales, favoreciendo que cada vez más personas en el mundo utilicen esta infraestructura en su vida cotidiana.

En la próxima etapa de nuestro desarrollo, los innovadores usarán Internet como punto de inicio para sus esfuerzos, creando nuevos productos y servicios diseñados específicamente para aprovechar las capacidades de la red. Mientras los desarrolladores empujan los límites de lo posible, las capacidades de las redes interconectadas que forman (Internet)* tendrán una función cada vez más importante en el éxito de esos proyectos.

En un futuro no muy lejano todas las transacciones que se realicen, el funcionamiento de la industria, las nuevas formas y métodos de enseñanza, la gestión política, las relaciones comerciales, los nuevos ámbitos del entretenimiento, el suministro de los servicios de salud y la comunicación con otras personas, se basarán en infraestructuras de red, llegaremos a un punto tal que nuestra vida estará rodeada de ellas, es algo inevitable, será asombroso, será el resultado del avance tecnológico, del desarrollo humano; todo esto parte de vivir en un mundo globalizado. Es un privilegio, entonces, para nosotros ser protagonistas y testigos de esta nueva era de cambios tan vertiginosos, esta nueva era que sin temor a exagerar podemos llamar **la era de la información**.

2. Antecedentes Históricos de la Computadora

2.1 Personajes siglos XIX y XX

Charles Babbage (**1791-1871**). Matemático británico y científico de la computación. Considerado por algunos como el padre de las computadoras modernas. Descubrió que se daban graves errores en el cálculo de tablas matemáticas. Intentó encontrar un método por el cual pudieran ser calculadas automáticamente por una máquina, eliminando errores debidos a la fatiga o aburrimiento que sufrían las personas encargadas de compilar tablas matemáticas de la época. En 1822 presentó un modelo que llamó **máquina diferencial** en la *Royal Astronomical Society*, se aprobó su idea y fue apoyado su proyecto. Entre 1833 y 1842 lo intentó de nuevo; esta vez, intentó construir una máquina que fuese programable para hacer cualquier tipo de cálculo. Esta fue la **máquina analítica**. El diseño se basaba en el telar de Joseph Marie Jacquard (1752 – 1834). La máquina analítica tenía dispositivos de entrada basados en las tarjetas perforadas de Jacquard, un procesador aritmético, una unidad de control, un mecanismo de salida y una memoria. Se considera que esta máquina fue la primera computadora del mundo. Un diseño inicial plenamente funcional de ella fue terminado en 1835. Lady Ada Lovelace, matemática e hija de Lord Byron, se enteró de los esfuerzos de Babbage y se interesó en su máquina. Promovió activamente la máquina analítica, y escribió varios programas para ella. Los diferentes historiadores concuerdan que esas instrucciones hacen de Ada Lovelace la primera programadora de computadoras en el mundo.

Ada Augusta Byron King (1815-1852). Única hija legítima del poeta inglés Lord Byron y de Annabella Milbanke Byron. Es conocida principalmente por haber escrito una descripción de la máquina analítica de Charles Babbage. Actualmente es considerada como la primera programadora, desde que escribió la manipulación de los símbolos, de acuerdo a las normas para esta máquina que aún no había sido construida. También preveía la capacidad de las computadoras para ir más allá de los simples cálculos de números, mientras que otros, incluido el propio Babbage, se centraron únicamente en estas capacidades.

George Boole (**1815-1864**). Matemático y filósofo británico, inventor del álgebra de Boole, la base de la aritmética computacional moderna. Boole es considerado como uno de los fundadores del campo de las Ciencias de la Computación. En 1854 publicó "*An Investigation of the Laws of Thought*" en él desarrollaba un sistema de reglas que le permitía expresar, manipular y simplificar, problemas lógicos y filosóficos cuyos argumentos admiten dos estados (verdadero o falso) por procedimientos matemáticos. Se podría decir que es el padre de las operaciones lógicas y gracias a su álgebra hoy en día podemos manipular este tipo de operaciones.

Herman Hollerith (**1860-1929**). Estadístico inventor de la máquina tabuladora. Es considerado como el primer informático, es decir, el primero que logra el tratamiento automático de la información. Hollerith comenzó a trabajar en el diseño de una máquina tabuladora o censadora, basada en tarjetas perforadas. El gobierno estadounidense eligió su máquina tabuladora para elaborar el censo de 1890. Se tardaron sólo 3 años en perforar unos 56 millones de tarjetas. Hollerith patentó su máquina en 1884. En 1896, fundó la empresa *Tabulating Machine Company*, con el fin de explotar comercialmente su invento. En 1911, dicha compañía se fusionó con *Dayton Scale Company, International Time Recording Company* y *Bundy Manufacturing Company*, para crear *la Computing Tabulating Recording Company* (CTR). El 14 de febrero de 1924, CTR cambió su nombre por el de *International Business Machines Corporation* (IBM).

Alan Mathison Turing (**1912-1954**). Matemático, informático, criptógrafo y filósofo inglés. Es considerado uno de los padres de la Ciencia de la Computación siendo el precursor de la informática moderna. Proporcionó una influyente formalización de los conceptos de algoritmo y computación: la **máquina de Turing**. Formuló su propia versión de la hoy ampliamente aceptada **Tesis de Church-Turing**, la cual postula que cualquier modelo computacional existente tiene las mismas capacidades algorítmicas, o un subconjunto, de las que tiene una máquina de Turing. Durante la Segunda Guerra Mundial, trabajó en romper los códigos nazis, particularmente los de la máquina **Enigma**. Tras la guerra diseñó uno de los primeros computadores electrónicos programables digitales en el Laboratorio Nacional de Física del Reino Unido y poco tiempo después construyó otra de las

primeras máquinas en la Universidad de Manchester. Entre otras muchas cosas, también contribuyó de forma particular e incluso provocadora al debate de si las máquinas pueden pensar, es decir al debate relativo a la Inteligencia Artificial.

Konrad Zuse (**1910-1995**). Ingeniero alemán. En 1938 hizo su primer intento de construir una máquina programable llamada **Z1**, nunca funcionó bien debido a que no tenía suficiente precisión en sus componentes. La Z1 y sus planos originales fueron destruidos durante la Segunda Guerra Mundial. En 1939 Zuse fue llamado al servicio militar, sin embargo, logró convencer al ejército de que lo dejaran regresar a construir sus computadoras. En 1940 Zuse construyó la **Z2**, una versión mejorada de su primera máquina, a partir de relevadores o "relés" telefónicos. Ese mismo año, fundó una compañía la *Zuse Apparatebau* (Ingeniería de Aparatos Zuse), para manufacturar sus computadoras programables. Satisfecho con la funcionalidad básica de la máquina Z2, inició la construcción de la **Z3** que terminó en 1941, era una calculadora binaria que se programaba con ciclos pero sin saltos condicionales, con memoria y una unidad de cálculo basada en los mencionados relevadores telefónicos. A pesar de la ausencia de saltos condicionales como instrucciones convenientes, la Z3 era una **computadora Turing** completa (ignorando el hecho de que ninguna computadora física puede ser verdaderamente Turing completa debido a su limitada capacidad almacenamiento). Sin embargo, Zuse nunca pudo ver en su totalidad esta característica de la computadora Z3 (ya que tenía en mente sólo sus aplicaciones prácticas) la cual fue demostrada a finales de ese siglo.

La compañía de Zuse fue destruida en 1945 por un ataque aliado, junto con la Z3. La **Z4** estaba parcialmente terminada, se basada en relevadores mejorados y había sido llevada a un lugar más seguro con anterioridad. Zuse diseñó un lenguaje de programación de alto nivel llamado **Plankalkül** entre 1941 y 1945. Ningún compilador o intérprete estuvo disponible para el Plankalkül hasta que un equipo de la Universidad Libre de Berlín lo implementó en el año 2000, cinco años después de la muerte de Zuse.

Howard H. Aiken (**1900-1973**). Ingeniero estadounidense. Estudio en la Universidad de Wisconsin-Madison, y posteriormente obtuvo su doctorado en física en la Universidad Harvard en 1939. Durante este tiempo, encontró ecuaciones diferenciales que sólo se podían resolver numéricamente. Ideó un dispositivo

electromecánico de computación que podía hacer gran parte de ese trabajo por él. Esta computadora fue originalmente llamada *Automatic Sequence Controlled Calculator* (**ASCC**), posteriormente renombrada **Harvard Mark I**. Con la ayuda de Grace Hopper y financiación de IBM, la máquina fue completada en 1944.

La Mark I fue el primer ordenador electromecánico construido en la Universidad Harvard en 1944, con la subvención de IBM. Tenía 760.000 ruedas y 800 kilómetros de cable y se basaba en la máquina analítica de Charles Babbage. La computadora Mark I empleaba señales electromagnéticas para mover las partes mecánicas. Esta máquina era lenta (tomaba de 3 a 5 segundos por cálculo) e inflexible (la secuencia de cálculos no se podía cambiar); pero ejecutaba operaciones matemáticas básicas y cálculos complejos de ecuaciones sobre el movimiento parabólico de proyectiles. Funcionaba con relés, se programaba con interruptores y leía los datos de cintas de papel perforado.

En 1947, Aiken completó su trabajo en el ordenador **Harvard Mark II**. Continúo su trabajo en el **Harvard Mark III** y en el **Harvard Mark IV**. El Mark III utilizó algunos componentes electrónicos y el Mark IV fue completamente electrónico, ambos utilizaron memoria de tambor magnético y el último también tenía un núcleo de memoria magnética. Vivió en México en el estado de Puebla. En 1970, Aiken recibió la Medalla Edison del IEEE por una meritoria carrera de contribuciones pioneras al desarrollo y la aplicación de computadoras digitales de gran escala e importantes contribuciones a la educación en el campo de las computadoras digitales.

John von Neumann (**1903-1957**). Retomando el proyecto ENIAC, desarrolló el concepto de **programa almacenado**, lo que permitió la lectura de un programa dentro de la memoria de la computadora, característica que se implementó en la computadora llamada **EDVAC** (*Electronic Discrete-Variable Automatic Computer*) desarrollada en conjunto con, **John Presper Eckert** y **John William Mauchly**. Los programas almacenados dieron a las computadoras flexibilidad y confiabilidad, haciéndolas más rápidas y menos sujetas a errores que los programas mecánicos. Esto dio paso a la arquitectura que lleva su nombre (arquitectura von Neumann), utilizada en casi todas las computadoras. Virtualmente, cada computadora personal, microcomputadora, minicomputadora y supercomputadora es una **máquina Von Neumann**.

2.2 Primeras Computadoras

Computadoras ENIAC, EDVAC y UNIVAC

En 1943 surgió el proyecto **ENIAC** (*Electronic Numerical Integrator and Computer*) construida en la Universidad de Pennsylvania, encabezado por **John Presper Eckert** y **John William Mauchly**, el primero era ingeniero responsable del proyecto cuya tarea principal era diseñar sus circuitos eléctricos. Fue la primera computadora de propósito general, era totalmente digital, es decir, que ejecutaba sus procesos y operaciones mediante instrucciones en **lenguaje máquina**, a diferencia de otras máquinas computadoras contemporáneas de procesos analógicos. La ENIAC podía resolver problemas que hasta entonces no eran se habían planteado. Era más veloz que las computadoras creadas hasta entonces. Podía sumar cinco mil números o hacer catorce multiplicaciones de diez dígitos en un segundo.

Mención especial merecen seis mujeres que se ocuparon de programar la ENIAC, cuya historia ha sido silenciada a lo largo de los años y recuperada en las últimas décadas. Clasificadas entonces como "sub-profesionales", posiblemente por una cuestión de género o para reducir los costos laborales. El equipo era conformado por **Betty Snyder Holberton**, **Jean Jennings Bartik**, **Kathleen McNulty Mauchly Antonelli**, **Marlyn Wescoff Meltzer**, **Ruth Lichterman Teitelbaum** y **Frances Bilas Spence**, las cuales eran hábiles matemáticas y lógicas que trabajaron inventando la programación a medida que la realizaban, estas mujeres sentaron las bases para que la programación fuera sencilla y accesible para todos, crearon el primer *set* de rutinas, las primeras aplicaciones de software y las primeras clases en programación. Su trabajo modificó drásticamente la evolución de la programación entre 1940 y 1960.

En 1941 se construye la **UNIVAC I** (*Universal Automatic Computer I*) primera computadora comercial fabricada en Estados Unidos, diseñada también por Eckert y Mauchly. Durante los años previos a la aparición de sus sucesoras, la máquina fue simplemente conocida como **UNIVAC**. Se donó un ejemplar a la Universidad de Harvard y otro a la Universidad de Pensilvania. Fue la primera computadora fabricada para un propósito no militar. Además de ser la primera computadora comercial estadounidense, el UNIVAC I fue la primera computadora diseñada desde

el principio para su uso en administración y negocios, es decir, para la ejecución rápida de grandes cantidades de operaciones aritméticas relativamente simples y transporte de datos, a diferencia de los cálculos numéricos complejos requeridos por las computadoras científicas.

De estos proyectos, algunos exitosos y otros no, algunos terminados y otros inconclusos, se desprende el desarrollo de las tecnologías de la información, llegando a ser hasta nuestros días una herramienta vital en nuestra vida cotidiana.

Computadora Atlas

La computadora Atlas fue desarrollada en conjunto por la Universidad de Manchester y *Ferranti International* y *Plessey Company*. Empezó a funcionar en 1962 y fue una de los primeras supercomputadoras del mundo. Se decía que cada vez que ésta se desconectaba, la mitad de la capacidad de procesamiento de información del Reino Unido se perdía. Era una máquina de segunda generación y usaba transistores de germanio en lugar de tubos de vació.

Otras tres máquinas Atlas fueron construidas, una para la *British Petroleum*, otra para la Universidad de Londres y otra para el Laboratorio Atlas de Informática en Chilton, cerca de Oxford. Un sistema similar fue construido por *Ferranti* para la Universidad de Cambridge, llamado el **Titán** o **Atlas 2**. Tenía una organización de memoria diferente y un sistema operativo de tiempo compartido desarrollado por el *Cambridge Computer Laboratory*. El Atlas de la Universidad de Manchester fue deshabilitado en 1971, sin embargo, el último estuvo en servicio hasta 1974.

Computadora Altair 8800

La Altair 8800 creada por **Henry Edward Roberts** y **Forrest M. Mims III** a través de su empresa MITS (*Micro Instrumentation and Telemetry System*) fue una microcomputadora diseñada en 1975, basada en la CPU Intel 8080A. Hoy en día, la Altair 8800 es ampliamente reconocida como piedra angular para la industria de las

computadoras personales. El bus de computador diseñado para la Altair 8800 se convirtió en un estándar de facto conocido como el Bus S-100.

En el primer diseño de la Altair 8800, las partes necesarias para hacer una máquina completa no cabían en una sola **tarjeta madre**. La máquina consistía en cuatro tarjetas apiladas una encima de la otra con unos separadores. Durante la construcción del segundo modelo, se decidió construir la mayor parte de la máquina en forma de tarjetas extraíbles, reduciendo la tarjeta madre a nada más que una interconexión entre las tarjetas, un ***backplane***. La máquina básica consistió en cinco tarjetas, incluyendo la CPU en una y la memoria en otra.

Programar la Altair 8800 era un proceso extremadamente tedioso, entonces se utilizaba un interruptor especial para introducir el código en la memoria de la máquina, y después repetir este paso hasta que todos los ***opcodes*** de un programa probablemente completo y correcto estaban en su lugar. Cuando la máquina se despachó por primera vez, los interruptores y las luces eran la única interfaz, todo lo que se podía hacer con la máquina eran programas para que las luces centellearan. Sin embargo, muchas fueron vendidas en esta forma. **Ed Roberts** estaba trabajando duro con tarjetas adicionales, incluyendo un lector de cinta de papel para el almacenamiento, tarjetas adicionales de memoria RAM, y una interfaz RS-232 para conectarse a una terminal apropiada. Bill Gates y Paul Allen diseñaron el leguaje de programación para la Altair 8800 el cual fue llamado **Altair BASIC** el cual funcionó al primer intento, este evento motivó a Gates y a Allen a crear *Microsoft Corporation*.

3. Precursores de Internet

3.1 Personajes siglos XX y XXI

Joseph Carl Robnett Licklider (1915-1990). Comúnmente conocido como J.C.R. Licklider. Fue un científico americano de la computación, considerado como uno de las más importantes figuras en las ciencias de la computación y en la historia de la computación en general. Nació en St. Louis, Missouri, EU. Demostró tempranamente su talento de ingeniero, construyendo modelos de aeroplanos. Estudió en la Universidad de Washington en San Luis, donde recibió en 1937 un BA (*Bachelor of Arts*), se especializó en física, matemáticas y psicología, en 1938 obtuvo el grado de Maestro en Psicología. En 1942 finalizó su Doctorado en Psicoacústica en la Universidad de Rochester, Nueva York y trabajó en el Laboratorio de Psicoacústica de la Universidad de Harvard de 1943 a 1950.

Tuvo un gran interés en las tecnologías de la información trasladándose en 1950 al MIT (*Massachusetts Institute of Technology*) como profesor asociado, donde participó en el comité para fundar el Laboratorio Lincoln en el MIT y estableció un programa de psicología destinado a estudiantes de ingeniería. En 1957 recibió el premio Franklin V. Taylor otorgado por la Sociedad de Ingenieros Psicólogos.

En 1958, fue elegido Presidente de la Sociedad Acústica de América, y en 1990 recibió el *Commonwealth Award for Distinguished Service*. En octubre de 1962, Licklider fue nombrado jefe la Oficina de Técnicas y Procesamiento de Información (IPTO, *Information Processing Techniques Office*) de ARPA. En 1963, fue nombrado Director del Comando de las Ciencias del Comportamiento e Investigación de Control (*Behavioral Sciences Command & Control Research*) de ARPA.

En abril del mismo año, envió un memorándum a sus colegas en el cual esboza los primeros desafíos presentados al tratar de establecer una red de tiempo compartido entre computadoras con el software de esa época. Esta era la visión de ARPANET, la precursora de la Internet actual.

En 1968, J.C.R. Licklider se convirtió en director del Proyecto MAC del MIT, y profesor en el Departamento de Ingeniería Eléctrica del mismo. El Proyecto MAC

produjo el sistema de computadora de tiempo compartido (CTSS, *Computer Time-Sharing System*), y el primer sistema de configuracion en línea con el desarrollo de Multics (trabajo que comenzó en 1964). Multics proveyó la inspiración de algunos elementos del Sistema Operativo Unix desarrollado en los Laboratorios Bell por **Ken Thompson** and **Dennis Ritchie** en 1970.

Licklider se interesó por la tecnología de la información al principio de su carrera. Al igual que **Vannevar Bush**, J.C.R. Licklider contribuyó al desarrollo de la Internet con ideas consistentes, no invenciones. Previó la necesidad de computadoras conectadas en red con interfaces de usuario. Predijo ideas y conceptos acerca de la computación gráfica, las interfaces con un apuntador (hacer "clic"), las bibliotecas digitales, el comercio electrónico, la banca en línea, y software diverso que existe hoy en día, hasta el concepto de migración de datos en caso de ser necesario.

Licklider fue fundamental en la concepción, financiación y gestión de la investigación que condujo a las modernas computadoras personales e Internet.

Su artículo publicado en 1960 sobre la "Simbiosis Hombre-Computadora" ("*Man-Computer Symbiosis*") anunciaba el cómputo interactivo. Concentró sus mayores esfuerzos en el concepto de tiempo compartido y en el desarrollo de aplicaciones. Licklider formuló las primeras ideas de una red de computadoras mundial en agosto de 1962 en BBN, en una serie de notas que discutían el concepto de "Red Galáctica" ("*Galactic Network"*). Estas ideas contenían todo lo que internet es hoy en día. En 1968 publica su artículo "La Computadora como Dispositivo de Comunicación" ("*The Computer as a Communication Device"*) donde expone la idea del uso de redes informáticas para apoyar a las comunidades con intereses comunes, y que a su vez colaboraran entre sí, sin importar en dónde se ubicaran.

Se retiró convirtiéndose en Profesor Emérito en 1985. Murió en 1990 en Arlington, Massachusetts. Tiene el reconocimiento histórico por haber plantado las semillas de la informática en la era digital.

Leonard Kleinrock (1934). Ingeniero y distinguido profesor de ciencias de la computación en la Escuela de Ingeniería y Ciencias Aplicadas Henry Samueli, de la Universidad de California, Los Ángeles, (UCLA). Coadyuvó de manera imprescindible en el desarrollo de la actual Internet, contribuyendo en diversas áreas de las redes de computadoras.

Vivió sus primeros años en Manhattan con sus padres. Su primera creación tuvo lugar cuando era niño, fabricando un radio de cristal, inspirado por un cómic de Superman donde en la parte central se hallaban los pasos para la construcción de este radio. Los próximos años se dedicó a perfeccionar sus habilidades en radios electrónicos. Durante sus primeros estudios profesionales trabajo medio tiempo cómo técnico en electrónica para poder llevar un poco de dinero a su familia.

Después de obtener su Licenciatura, ganó una beca para estudiar el Posgrado. Realizó su educación media superior en la legendaria Bronx High School de Ciencias en 1951, obtuvo su Licenciatura en Ingeniería Eléctrica en 1957 en el City College de Nueva York, continuó con sus estudios de maestría y doctorado en Ingeniería Eléctrica en el Instituto Tecnológico de Massachusetts (MIT), en 1959 y 1963, respectivamente. Entre 1991 y 1995 fue catedrático del Departamento de Ciencias de la Computación.

Desarrolló la teoría matemática de las **redes de paquetes** y fue responsable de uno de los primeros 4 nodos de ARPANET en la Universidad de California, Los Ángeles. Su obra más conocida y significativa es su trabajo en teoría de colas, que tiene aplicaciones en una multitud de campos, entre ellos como fundamento matemático de la conmutación de paquetes, tecnología básica detrás de Internet. Su contribución inicial en este campo fue su propuesta de tesis doctoral “Flujo de Información en la Comunicación de una Gran Red” (*"Information Flow in Large Communication Nets"*) en julio de 1961, publicada en 1964.

Finalmente su tesis doctoral se llamó “Retraso de Mensajes en Redes de Comunicación con Almacenamiento” (*“Message Delay in Communication Nets with Storage”*) en 1962. Más tarde publicaría diversas obras de referencia en la materia. Ha descrito su trabajo de la siguiente manera*:* “*Básicamente, lo que hice en mi*

investigación de tesis doctoral entre 1962 y 1964 fue establecer una teoría matemática de las redes de paquetes..."

Su trabajo teórico en el campo del encaminamiento jerárquico, realizado a finales de los 70's con su estudiante Farouk Kamoun, juega un papel crítico en la actualidad en la operación de Internet. Actualmente, continúa impartiendo clases en el Departamento de Ciencias de la Computación en la Universidad de California, Los Ángeles.

Robert Taylor (1932). Una de las mayores figuras del desarrollo de la Internet. Nació en Dallas, Texas, hijo de un ministro metodista y pasó una niñez de parroquia en parroquia. Ingreso a la Universidad Metodista del Sur a los 16 años, sirvió a la Marina durante la Guerra de Corea, y posteriormente se incorporó a la Universidad de Texas. Realizó estudios en psicología experimental, matemáticas, filosofía y religión. Dedico sus investigaciones primarias al funcionamiento cerebral y al sistema auditivo nervioso. Apoyo en la logística a su país durante la Guerra de Vietnam.

Taylor se unió a la NASA en 1961 y coadyuvó en la administración del Presidente John F. Kennedy post-Sputnik, con la intención de llevar al hombre a la luna. En 1963 Robert conoció a J.C.R. Licklider. Pasa de la NASA a la ARPA, y como director de ésta financia programas de investigación avanzada en informática en todo el país. En 1968 publica junto con Licklider un artículo titulado "La computadora como un dispositivo de comunicación" que iniciaba diciendo "*en poco años, el hombre se comunicará más eficientemente a través de una computadora que cara a cara".*

Como gerente de investigación de la NASA, Taylor financió el trabajo de Douglas C. Engelbart que derivó en el desarrollo del ratón de computadora. De 1965 a 1969 fue director de la Oficina de Técnicas de Procesamiento de Información (IPTO*, Information Proccesing Techniques Office*), fundador y posteriormente director del Laboratorio de Ciencias de la Computación (CLS) en el Centro de Investigación de la Corporación Xerox en Palo Alto, California (*Xerox PARC's Computer Science Laboratory*) de 1970 a 1983; además fundador y director del Centro de Investigación

en Sistemas (SRC) de la *Digital Equipment Corporation's Systems Research Center* de 1983 a 1996.

Su trabajo fue reconocido en varias ocasiones. En 1999 se le otorgó la Medalla Nacional de Tecnología por su liderazgo visionario en el desarrollo de la tecnología informática moderna, incluyendo la iniciación del proyecto ARPANET y el avance revolucionario en el desarrollo de las computadoras personales y redes informáticas. En 2004, la Academia Nacional de Ingeniería le otorgó, junto con Butler W. Lampson, Charles P. Thacker y Alan Kay su máximo galardón, el Premio Draper, por la visión, concepción y desarrollo de las primeras prácticas de computadoras personales en red. Taylor está retirado y vive actualmente en California.

Douglas Engelbart (1925). Inventor americano. Mejor conocido como el invento del ratón de computadora. Nació en Oregon, Estados unidos. Descendiente de alemanes, suizos y noruegos. Vivió en Portland sus primeros años. En 1942 concluyó su educación media superior en el Colegio Franklin en Portland. Cursó la mitad de sus estudios profesionales en la Universidad Estatal de Oregon. Justo al finalizar la Segunda Guerra Mundial, se integró a la Armada, cumplió dos años como técnico en radar en Filipinas. Regresó a Oregon y finalizó su licenciatura en Ingeniería Eléctrica en 1948, realizó un posgrado en Ingeniería Eléctrica con especialidad en Computadoras en 1953 y un doctorado en la misma área en 1955, ambos en la Universidad de California en Berkeley (UCB). En 1994 le otorgaron el grado de Doctor Honorario por parte de la Universidad del Estado de Oregon y de manera similar la Universidad de Santa Clara en el año 2001. Como estudiante graduado de UCB colaboró en la construcción del proyecto Computadora Digital California (*CALDIC*, *California Digital Computer*), al finalizar su doctorado continuó impartiendo clases en esta Universidad.

Douglas había leído sobre computadoras (un fenómeno relativamente reciente), y con su experiencia como técnico de radar, sabía que la información puede ser analizada y mostrada en una pantalla. De repente se imaginó trabajadores intelectuales sentados enfrente de una pantalla, los “lugares de trabajo” volando por el espacio de información, el aprovechamiento de su capacidad intelectual colectiva para resolver problemas de gran importancia de maneras mucho más poderosas. Aprovechar la inteligencia colectiva, facilitada por equipos interactivos; todo esto se

convirtió en la misión de su vida en un momento cuando las computadoras eran vistas como herramientas de procesamiento de números.

Dejó la universidad de Berckeley para realizar su "visión", después de un año de profesorado, y se integro al Instituto de investigación de Standford (SRI*, Standford Research Institute*) en Menlo Park, esperando poder realizar esa "visión" que tanto le inquietaba.

Patentó diversos resultados de sus investigaciones durante sus posgrados. Elaboró un informe sobre su visión y la agenda de investigación propuesta titulada "Aumentando el Intelecto Humano: Un Marco de Trabajo Conceptual" ("*Augmenting Human Intellect: A Conceptual Framework"*). Fundó el laboratorio llamado Centro de Investigación de Aumento (ARC, *Augmentation Research Center*), dentro del SRI, contrató a un equipo de investigación el cual se convirtió en la fuerza motriz detrás del diseño y desarrollo del Sistema en Línea (NLS, *oN-Line System*). Junto con su equipo de investigación desarrollaron algunos elementos de interfaz de computadora como las pantallas de mapa de bits, el ratón, el hipertexto, herramientas colaborativas, y el precursor de la Interfaz Gráfica de Usuario (GUI, *Graphical User Interface*), esto último lo desarrollo de mejor manera a mediados de la década de 1960.

A finales de 1969, su ARC de SRI se involucró en el desarrollo de ARPANET, estableciendo el primer enlace de computadoras electrónicas entre el laboratorio de Leonard Kleinrock en la UCLA y el ARC. Esta fue la espina dorsal de Internet.

Fundó el Instituto Doug Engelbart en 1988, actualmente dirigido por su hija Cristina Engelbart. En la actualidad Engelbart dirige diversos programas que impulsan el desarrollo informático y ofrece conferencias en diversos museos e instituciones tecnológicas.

Lawrence G. Roberts (1937). Científico y jefe de la Agencia de Proyectos de Investigación Avanzada. Roberts y su equipo crearon la conmutación de paquetes y la ARPANET. Roberts nació y creció en Westport, Connecticut. Asistió al Instituto de Tecnología de Massachusetts, donde realizó su Licenciatura, Maestría y Doctorado en Ingeniería Eléctrica.

Después de recibir su Doctorado, Roberts continuó trabajando en el Laboratorio Lincoln del MIT. Inspirado por el artículo de 1962 "Red de Computadoras Intergaláctica" (*"Intergalactic Computer Network"*) publicado por J.C.R. Licklider, Roberts implantó la primera conexión entre computadoras que podían comunicarse a través de paquetes de datos, con base en el sistema de conmutación de paquetes que le había propuesto su compañero del MIT, Kleinrock. En 1965, Roberts conectó una computadora TX2 en Massachusetts con un Q-32 en California a través de una línea telefónica conmutada de baja velocidad, creando así la primera (aunque reducida) red de computadoras de área amplia jamás construida. A finales de 1966 Roberts, se trasladó a ARPA a desarrollar el concepto de red de computadoras y rápidamente confeccionó su plan para ARPANET, publicándolo en 1967. En 1966 se convirtió en el principal científico de ARPA. En 1973 Roberts abandona la agencia, para comercializar la tecnología naciente a través de la compañía Telenet Inc., fundada en 1973, la primera compañía en ofrecer servicios de conmutación de paquetes instalando una red pública (posteriormente se comercializaría su uso) y se desempeño como CEO desde su creación hasta 1980.

Posteriormente Roberts fue presidente de la Sistemas de Modo Transferencia Asíncrona (*ATM Systems*) de 1993 a 1998. Fue director y jefe de Oficina Técnica de *Caspian Networks*, abandonando el puesto en el 2004. Roberts es fundador y actualmente director de *Anagran Inc.*, donde supervisa proyectos de administración de flujo en red bajo el concepto "Calidad en el Servicio" ("*Quality of Service*") para Internet.

Ivan Edward Sutherland (1938). Científico de la computación, pionero en el desarrollo de gráficos por computadora y precursor de la actual Internet. Nació en Hartings, Nebraska. Su padre, un doctor en ingeniería civil, y su madre, maestra, le transmitieron el interés por la academia. Su materia favorita en secundaria fue Geometría, comentó que "*… si puedo imaginar todas las soluciones posibles de la figura, tengo una mayor oportunidad de encontrar la correcta".* Sutherland se describió a sí mismo como un pensador visual, de ahí el interés por las gráficas en computadora.

Realizó su doctorado en el MIT, cuya tesis fue “Sketchpad: Sistema de Comunicación Gráfica Hombre-Máquina” (“*Sketchpad: A Man-machine Graphical Communications System*”), la primera Interfaz Gráfica de Usuario.

En 1963 al terminar su doctorado, se integró a la Armada donde trabajo en la Agencia Nacional de Seguridad (NSA, *National Security Agency*) como ingeniero eléctrico. En los siguientes años, Sutherland fue transferido a ARPA donde se encargó de proyectos de investigación en conceptos de computación importantes, como el tiempo compartido y la inteligencia artificial.

De 1968 a 1974, Sutherland fue profesor de la Universidad de Utah. Tuvo destacados alumnos como Alan Kay, el creador del lenguaje *Smalltalk* (lenguaje de programación que permite realizar tareas de computación mediante la interacción con un entorno de objetos virtuales), Henri Gouraud inventor de la técnica de sombreado *Gouraud* (técnica usada en gráficos 3D por computadora que simula efectos de luz y color sobre superficies de objetos), Frank Crow quien desarrollo el método *antialiasing* (técnica que reduce al mínimo los efectos de la distorsión conocida como *aliasing* al mostrar una imagen de alta resolución con una resolución menor) y Edwin Catmull, científico en gráficos por computadora, co-fundador de los estudios de animación Pixar y nuevo presidente de los estudios de animación de Walt Disney.

Posteriormente se integró como académico a la Universidad de Harvard. Dos años más tarde, se convirtió en profesor de la Universidad de Utah, construyendo una gran reputación en el área de gráficas por computadora. En 1976, Sutherland se desempeña como cabeza del Departamento de Ciencias de la Computación en el Tecnológico de California. Ahí ayudó al diseño de un circuito integrado. Hasta entonces, el diseño de circuitos integrados se consideraba demasiado difícil. Sin embargo, continúo en esta área impulsando la fabricación del chip en Sillicon Valley. Sutherland continúa como investigador en hardware de tecnología avanzada, específicamente en sistemas asíncronos.

Actualmente el Dr. Sutherland es líder en la investigación de sistemas asíncronos y fundador del Centro de Investigación Asíncrono (ARC, *Asynchronous Research Center*) en la Universidad Estatal de Portland.

Robert Elliot Khan (1938). Ingeniero y científico de la computación quien, junto con Vinton G. Cerf, inventó el Protocolo de Control de Transmisión (TCP, *Transmission Control Protocol*), el Protocolo de Internet (IP, *Internet Protocol*) y las tecnologías usadas para transmitir información sobre Internet.

Obtuvo su licenciatura en Ingeniería Eléctrica en el Colegio de la Ciudad de Nueva York en 1960, realizó su maestría y doctorado en la Universidad de Princeton en 1962 y 1964, respectivamente. Trabajo en los Laboratorios Bell AT&T, y se convirtió en profesor asistente en el MIT. Después ingresó a la compañía Bolt, Beranek and Newman (BBN), donde coadyuvó en el desarrollo del Procesador de Interfaz de Mensajes (Interface Message Processor).

En 1972, comenzó su trabajo en la IPTO en ARPA. A finales de 1972 tuvo lugar la Conferencia de Comunicación con Computadoras, dónde demostró el funcionamiento de la ARPANET que para entonces contaba con 20 computadoras conectadas, además que la conmutación de paquetes era una tecnología real. En ese tiempo ayudó a desarrollar el protocolo TCP/IP para implantarlo en las redes de computadoras. Más tarde fue nombrado Director de la IPTO, donde desarrolló el proyecto Iniciativa Computacional Estratégica (*Strategic Computing Initiative*), el más grande programa de investigación y desarrollo jamás realizado y financiado con cuantiosos recursos por el gobierno de los Estados Unidos.

Mientras trabajaba en el proyecto de una red de paquetes satelital, tuvo la idea de lo que más tarde se convirtió en el TCP (*Transmission Control Protocol)*, que fue pensado para remplazar un protocolo ya existente llamado Programa de Control de Red (NCP, *Network Control Program*) usado por ARPANET. Paralelamente a este proyecto, empezó a sentar las bases para las redes de arquitectura abierta (*open-architecture networking*), las cuales podrían permitir que las computadoras y las redes de ellas alrededor del mundo se comunicaran entre sí, sin importar que hardware o software se usara en cada red.

Para alcanzar este objetivo, TCP fue diseñado con las siguientes características:

- Pequeños segmentos en toda la red que permitan a las computadoras comunicarse unas con otras a través de una computadora especializada para solamente enviar paquetes (inicialmente llamado ***gateway***, ahora conocido como ***router***).
- Cualquier parte de la red puede fallar, y ésta no dejará de funcionar cuando ocurra algún problema. Ninguna parte de la red tiene el control total del funcionamiento.
- Cada segmento de información enviado a través de la red contará con un **número de secuencia**, para asegurarse que se recibieron correctamente en el equipo destino y detectar la pérdida de cualquiera de los segmentos.
- El equipo que envía la información, sabrá que fue recibido con éxito el paquete, cuando el equipo destino devuelva un paquete especial llamado **acuse de recibo** por cada pieza particular de información.
- Si la información enviada se perdió, la información se retransmite, esta pérdida es detectada cuando se agota un **tiempo de espera**, que indica que el acuse de recibo no fue recibido.
- Cada pieza de información envidada a través de la red deberá ir acompañada de una **suma de comprobación** calculada por el emisor original, y comprobada por el receptor final, para asegurarse de que la información no se dañó de alguna manera durante el trayecto.

Vinton Cerf se unió al proyecto en la primavera de 1973, y juntos completaron una primera versión de TCP. Posteriormente el protocolo se separa en dos capas, surgiendo el Protocolo de Internet (IP), que en la actualidad siguen siendo la base de la internet moderna.

Después de pertenecer por 13 años a la ARPA, abandona su cargo para fundar la Corporación de Iniciativas de Investigación Nacional (CNRI, *Corporation for National Research Initiatives*) en 1986. CNRI es una organización sin fines de lucro cuyo objetivo es proporcionar liderazgo y financiamiento para la investigación y el desarrollo de la Infraestructura de Información Nacional (*National Information Infrastructure*).

Fue galardonado en 1993 con el Premio SIGCOMM otorgado por el Grupo de Interés Especial de la Asociación de Maquinaria Computacional por su liderazgo y contribución en el desarrollo de las tecnologías en sistemas de información. En 2001 se convierte en miembro de la Asociación de Maquinaria de Cómputo. Compartió, en el año 2004, el Premio Turing con Vinton Cerf, por su trabajo en la creación de las redes y los protocolos básicos de comunicación, entre otros. En el año 2006 se integró, junto con Cerf, como Miembro Honorario de la Sociedad para la Comunicación Técnica (STC, *Society for Technical Communication*). Ambos recibieron el Premio Harold Pender, un galardón muy importante otorgado por la Escuela de Ingeniería y Ciencias Aplicadas de la Universidad de Pennsylvania, en 2010.

Ha recibido también varios Doctorados Honorarios de múltiples universidades, por ejemplo; la universidad de Princeton, Universidad de Pavia, Universidad Tecnológica Federal de Zurich (ETH Zurich), Universidad de Maryland, Universidad George Mason, Universidad Central de Florida y la Universidad de Pisa, además de ser Miembro Honorario del Colegio Universitario de Londres.

Vinton Cerf (1943). Científico americano de la Computación. Sus contribuciones han sido reconocidas con grados honorarios, y premios que incluyen la Medalla Nacional de Tecnología, el Premio Turing, la Medalla Presidencial de la Libertad, y es miembro de la Academia Nacional de Ingeniería. Cerf fue jefe de la ARPA, creando varios grupos para el avance en el desarrollo de la tecnología TCP/IP.

Durante la transición de la Internet al área comercial, en la década de 1980, Cerf ingresa al MCI Communications Corp., donde se integró al proyecto del desarrollo del primer sistema de correo electrónico comercial conectado a Internet.

Vinton Cerf fue pieza clave en la formación de la Corporación para la Asignación de Números y Nombres en la Internet (ICANN, *Internet Corporation for Assigned Names and Numbers*), llegando a ser presidente de la corporación.

Cerf ha trabajado para Google como su Vicepresidente y Jefe de Evangelización de Internet desde septiembre de 2005. Posee gran fama por sus predicciones sobre cómo la tecnología afectará a la sociedad en el futuro, abarcando áreas como la

inteligencia artificial, el advenimiento de **IPv6** y la transformación de la industria de la televisión.

Realizó su licenciatura en ciencias matemáticas en la Universidad de Stanford, terminó su maestría y su doctorado en ciencias de la computación en la Universidad de California, Los Ángeles y es poseedor de varios doctorados honorarios de múltiples universidades.

Su primer trabajo lo obtuvo en la IBM, dejándola después de un tiempo para estudiar su maestría y su doctorado. Al terminar estos estudios, estuvo bajo la dirección del Profesor Gerald Estrin, trabajó en el proyecto de paquetes de datos del profesor Leonard Kleinrock para conectar los dos primeros nodos de la ARPANET, contribuyendo a la creación del protocolo *host-to-host* de la misma. Durante su estancia en la UCLA, conoció a Robert Khan, quién había trabajado en la arquitectura a nivel hardware de ARPANET. Después de recibir su doctorado, se convirtió en profesor asistente en la Universidad de Stanford de 1972 a 1976, donde condujo la investigación de los protocolos de interconexión de redes de paquetes y co-diseñador de los protocolos TCP/IP del Departamento de Defensa de los Estados Unidos junto con Robert Khan. En 1976 se traslada a ARPA, donde permaneció hasta 1982.

Estuvo como vicepresidente de Servicios Digitales de Información MCI de 1982 a 1986, reingresó en 1994 y desempeñó el trabajo de vicepresidente *senior* de Estrategia Tecnológica, ayudando a llevar a cabo la misión corporativa desde una perspectiva técnica. Durante su estancia como vicepresidente *senior* en MCI, dirigió un equipo de arquitectos e ingenieros para diseñar característica de red avanzadas, incluidas soluciones basadas en Internet para ofrecer una combinación de datos, información, servicios de voz y video para uso profesional y de consumo.

Cerf en la actualidad forma parte del Consejo de Asesores de Científicos e Ingenieros de América para el gobierno de Estados Unidos, una organización centrada en la promoción de la ciencia del sonido, además, fue un importante contendiente para ser designado Primer Jefe de la Oficina de Tecnología de la nación para el gobierno del Presidente Barack Obama.

4. Historia de Internet

Origen de ARPA

La Agencia de Proyectos de Investigación Avanzada (ARPA) fue creada en febrero de 1958 en respuesta al lanzamiento del enlace satelital soviético *Sputnik*, en 1957, con la misión de mantener la tecnología militar de Estados Unidos a la vanguardia en la competencia tecnológica que sostenía con los enemigos de esa nación. ARPA, perteneciente al Departamento de Defensa de los Estados Unidos, realizó diversos experimentos con las redes de computadoras, involucrando posteriormente a organismos gubernamentales, universidades y compañías privadas en la investigación y desarrollo de estas tecnologías. El surgimiento de Internet tuvo lugar a finales de los sesenta como un experimento de la agencia. ARPA cambio su nombre por DARPA, incorporando la "D" por motivos de defensa, conservando este nombre hasta la actualidad.

Internet, una ilusión…

El concepto de "Red Galáctica" fue creado por J.C.R. Licklider, profesor e investigador del Instituto Tecnológico de Massachusetts (MIT). La visión de Licklider de una **red galáctica** "*una red de computadoras que permita a los usuarios recopilar datos y programas en cualquier parte del mundo*" fue detallado en una serie de publicaciones. El primer artículo se llamó "*Man-Computer Simbiosis*", fue escrito en 1960 y detalla reflexiones de Licklider sobre el desarrollo de la interacción entre humanos y computadoras. El segundo artículo "*On-Line Man Computer Communication*", fue publicado dos años más tarde. La idea principal era la de promover el concepto de **interacción social** a través de la creación de redes de computadoras. En 1968, Licklider fue coautor de "*The Computer as a Communication Device*" junto con el investigador Robert Taylor, en el cual discutía la idea de utilizar las comunidades en línea y los sistemas como un método eficaz de comunicación humana.

El concepto de “Red Galáctica” influyo significativamente en el desarrollo inicial de **ARPANET**.

En 1962, Licklider tomo el cargo de director de la Oficina de Técnicas de Procesamiento de Información (IPTO) subsidiada por ARPA, la cual financió investigaciones tecnológicas avanzadas para redes de computadoras, posteriormente, en octubre de 1963, Licklider fue nombrado jefe de las Ciencias del Comportamiento y de Mando y Control en los programas de ARPA. La visión de Licklider de una red universal tuvo gran influencia en sus sucesores en la IPTO, convenciendo a Ivan Sutherland, Bob Taylor y Lawrence G. Roberts de que una red informática mundial era un concepto de gran valor. Licklider dejó ARPA sin materializar alguna de ellas debido a su incorporación a IBM en julio de 1964, dejando la dirección a Ivan Sutherland, sin embargo, antes de salir de la IPTO convenció a Sutherland, a Robert Taylor, y a el investigador del MIT, Lawrence Roberts, de lo importante de su proyecto. Las siguientes investigaciones de estos científicos sucesores condujeron al desarrollo de la actual Internet.

En 1965 Sutherland concedió a Lawrence Roberts un contrato para seguir desarrollando la tecnología de redes de computadoras y avanzar en las investigaciones. En 1966, Sutherland cedió la dirección de IPTO a Robert Taylor, quien había sido fuertemente influenciado por las ideas de Licklider.

Taylor tenía tres terminales diferentes en su oficina en la IPTO para conectarse a tres centros de investigación, se percato que si mantenía esta arquitectura limitaría gravemente la escalabilidad, ya que cuando tenía comunicación con una institución y quería enviar un mensaje a otra, tenía que cambiarse de terminal. Esto motivó la idea de utilizar una sola terminal para hablar con las tres instituciones al mismo tiempo, pensó que con su puesto en el Pentágono podría ejercer presión para financiar la implementación de su visión.

En 1966 ARPA estaba encabezada por Charles M. Herzfeld la cual prometió un millón de dólares a la IPTO si lograba construir una red de comunicaciones distribuidas. En aquella época Taylor estaba impresionado por el trabajo de Roberts, y le pidió unir esfuerzos para el proyecto, sin embargo, Robert se resistió. Taylor le pidió a Hertzfeld la dirección de los Laboratorios Lincoln para poder convencer a

Roberts de la importancia de este propósito, logrando finalmente que se uniera a la IPTO como Jefe Científico en diciembre de 1966. Roberts presentó a Taylor a mediados de 1968 el informe titulado "**Uso Compartido de Recursos en Redes de Computadoras**", que describía la estructura general y las especificaciones para construir ARPANET.

En 1968 ya existía un plan completo para desarrollar ARPANET, por lo que esta institución lanzó un licitación para desarrollar el componente clave, la **conmutación de paquetes**, la cual en 1969 fue ganada por *Bolt, Beranek and Newman Corporation* (BBN), en donde el Ingeniero Robert E. Khan (llamado también, Bob Kahn) se unió al proyecto y jugó un papel preponderante en el diseño arquitectónico de ARPANET. La topología de red y el diseño módico fue trabajo de Roberts y Howard Frank, el sistema de medición de red fue diseñado por el equipo de Leornard Kleinrock de la Universidad de California, Los Ángeles (UCLA), este proyecto se basaba en los conceptos de conmutación de paquetes, aportados por el científico Donald Davies miembro del Laboratorio Nacional de Física (NPL) del Reino Unido.

A partir de este hecho comenzó la travesía de la creación de ARPANET, durante los 14 meses siguientes, siendo la primera red operacional de conmutación de paquetes. Esta tecnología era un concepto nuevo e importante la cual se había basado en la idea de la conmutación de circuitos. Esta comunicación se basada en el llamado Protocolo de Control de Red (NCP, *Network Control Protocol*), el cual permitía un flujo viable, controlado además de enlaces de comunicación bidireccional. La interfaz del software NCP permitía conectase a través de la ARPANET mediante los protocolos de mayor nivel, un ejemplo de estos era el modelo Interconexión de Sistemas Abiertos (OSI).

Cuando ARPANET estaba consolidada, Taylor, entregó el cargo de director de la IPTO a Roberts. Años más tarde Roberts renunció para convertirse en director ejecutivo de Telenet Inc., Licklider regresó de nuevo como director de la IPTO en octubre de 1973, para completar el ciclo de vida de la organización.

Nace Internet

ARPANET inició operaciones en agosto de 1969, cuando BBN entregó la primera Interfaz Procesadora de Mensajes (IMP, *Interface Message Processor*) al Centro de Medición de Red de UCLA el cuál fue seleccionado por su enfoque en el análisis, diseño y medición, cuyo responsable era el ingeniero Leonard Kleinrock. El equipo responsable para la instalación del IMP y la creación del primer nodo de ARPANET fueron los estudiantes graduados Vinton Cerf, Steve Crocker, Bill Naylor, Jon Postel y Mike Wingfield, quienes diseñaron la primera interfaz de hardware entre la computadora de UCLA y el IMP, las máquinas estaban conectadas, después de un par de días de prueba el IMP se conectó con el Centro de Medición de Red, el intercambio de mensajes era exitoso. ARPANET había nacido.

La primera demostración pública de ARPANET, tuvo lugar en la *International Computer Communication Conference* (ICCC) celebrada en Washington D.C., en octubre de 1972, la logística del evento corrió a cargo de Robert Kahn.

Infraestructura

En la primera fase, ARPANET estaba constituida por 4 IMPs.

1) **UCLA** (Universidad de California, Los Ángeles) en el NMC (Network *Measurement Center*). Computadora SDS Sigma 7. Sistema Operativo SEX.
2) **SRI** (Instituto de Investigación de Standford) en el ARC (*Augmentation Research Center*). Computadora SDS 940. Sistema Operativo Genie.
3) **UCSB** (Universidad de California, Santa Bárbara) en el IMC (*Interactive Mathematics Centre*). Computadora IBM 360. Sistema Operativo OS/MVT.
4) **UTAH** (Universidad de Utah). GB (*Graphics Department*). Computadora DEC PDP-10. Sistema Operativo Tenex.

Estos sitios iniciales fueron seleccionados por Roberts ya que tenían la capacidad técnica necesaria para desarrollar la interfaz personalizada para los IMPs.

El primer mensaje que se envía a través de ARPANET (enviado a través de la primera conexión host-a-host) se produjo a las 22:30 hrs, el 29 de Octubre de 1969 a una velocidad de 50 kbps y sobre una infraestructura de AT&T Telephone Company. Fue enviado desde la UCLA por un estudiante programador, Charley Kline, supervisado por el profesor Leonard Kleinrock (estudiante y profesor de la UCLA respectivamente) hacia el SRI. Días más tarde, el 21 de noviembre del mismo año, el enlace quedo establecido permanentemente. El 5 de diciembre de 1969, los cuatros nodos estaban conectados permanentemente y comunicándose entre sí a 50 Kbps correctamente.

Esto fue ARPANET, una red donde varias personas de diferentes instituciones podían comunicarse e intercambiar información entre sí de forma simultánea. En los años subsecuentes ARPANET creció rápidamente, sin embargo, tenía una Política de Uso Aceptable (AUP, *Acceptable Use Policy*) que prohibía el uso de internet para propósitos comerciales.

Para 1983 ARPANET ya se constituía de múltiples nodos, por lo que la División Militar de los Estados Unidos observó una potencial vulnerabilidad de su seguridad y decidió separar MILNET (*Military Network*) de ARPANET, esto facilitó el primer crecimiento de la red hacia el acceso público.

Crecimiento

En 1968 dos enlaces satelitales atravesaban el océano Pacífico y el océano Atlántico, de Hawái a Noruega. La Matriz Noruega Sísmica (NORSAR) había sido conectada a ARPANET. En Marzo de 1970, ARPANET llegó a la costa este de Estados Unidos, fue entonces cuando la compañía BBN se conecta a la red. En 1973 se instaló un circuito terrestre desde Noruega hacia el IMP de Londres, el cuál fue también incorporado a ésta. En 1974 Vinton Cerf y Bob Kahn publican "*A Protocol for Packet Network Interconnection*", que especifica en detalle el diseño del Programa de Control de Transmisión (TCP). En 1975 se transfiere el control de ARPANET a la Agencia de Comunicaciones de Defensa (DCA, *Defense Communications Agency*). En 1980 la Fundación Nacional de Ciencia (NSF,

National Science Foundation) crea CSNET (*Computer Science Network*), durante los próximos 5 años la NSF financió la mejora de la infraestructura computacional de CSNET y por lo tanto de las universidades.

El objetivo principal era incrementar la velocidad de conexión la red y aumentar la capacidad de las computadoras en los diferentes puntos de acceso de la CSNET ya que el nivel de investigación de estas instituciones lo demandaba. En 1985 comenzó la migración de CSNET a NSFNET (*National Science Foundation Network*) la cual llegó a poseer una velocidad de transmisión muy superior a su predecesora. A principios de 1986 NSFNET comienza operaciones y crece aceleradamente estableciendo conexiones con más universidades, instituciones de gobierno y por primera vez se abre la conexión a la industria privada.

Sin embargo, el objetivo principal de la NSFNET fue vincular a ARPANET los departamentos de ciencia e informática de diversas instituciones académicas con el objeto de que los investigadores, académicos y estudiantes, tuvieran acceso a supercomputadoras que facilitaran su trabajo, esto puso al descubierto los múltiples beneficios del trabajo en red, esto hizo evidente los problemas de escalabilidad para los puntos de conexión, de los que el más notable era la congestión de los enlaces, por lo que científicos e investigadores comenzaron el desarrollo de diversos protocolos para resolver distintos problemas en la comunicación. En 1983 el NCP es sustituido por el protocolo TCP/IP usado actualmente.

Desde sus inicios ARPANET creció aceleradamente al incorporarse múltiples nodos día con día. Para el año 1989 la cantidad de *host* superaba los 100,000. ARPANET deja de prestar servicios en 1990.

5. Fundamentos de comunicación y de redes de computadoras

Sistemas de comunicación

El objetivo principal de todo sistema de comunicación es intercambiar información entre dos entidades. Esto debido a la necesidad de hacer un uso eficaz de los recursos utilizados en la transmisión, los cuales se suelen compartir habitualmente entre una serie de dispositivos de comunicación. La capacidad total del medio se transmisión se reparte entre los distintos usuarios haciendo uso de técnicas denominadas de **multiplexación**. Además, se necesitan técnicas de control de congestión para garantizar que el sistema no se sature por una demanda excesiva de servicios de transmisión.

Para que un dispositivo pueda transmitir información tendrá que hacerlo a través de la interfaz con el medio de transmisión, esto depende de la utilización de señales electromagnéticas que se transmitirán a través del medio. Una vez que la interfaz esté establecida, será necesaria la generación de la señal, estas deben de permitir alguna forma de sincronización que cumplan con los requisitos del sistema de transmisión y del receptor. El receptor debe de ser capaz de determinar cuando comienza y cuándo acaba la señal recibida al igual que su duración. Si se necesita intercambiar datos durante un periodo de tiempo, las dos partes deben cooperar, por lo que necesitarán ciertas convenciones además del simple hecho de establecer la conexión.

En todo los sistemas de comunicación es posible la existencia de errores, ya que la señal transmitida sufre una degradación (por mínima que sea) antes de alcanzar su destino, por lo tanto, en circunstancias donde no se pueden tolerar los errores se necesitarán procedimientos para la detección y corrección de éstos. Para evitar que la fuente no sature el destino transmitiendo datos más rápidamente de lo que el receptor pueda procesar y absorber, se necesitan una serie de procedimientos denominados control de flujo. Cuando cierto recurso de transmisión se comparte con más de dos dispositivos, el sistema fuente deberá, de alguna manera, indicar la identidad del destino. El sistema de transmisión deberá garantizar que ese destino, y sólo ese, reciba los datos. En el sistema de transmisión puede existir más de un

camino para alcanzar el destino; en este caso se necesitará, la elección de una de entre las posibles rutas.

La recuperación es un concepto distinto a la corrección de errores. En ciertas situaciones en las que el intercambio de información se vea interrumpido por algún fallo, se necesitará un mecanismo de recuperación. Por otra parte, el formato de mensajes está relacionado con el acuerdo que debe existir entre las dos partes respecto al formato de los datos intercambiados, además, frecuentemente es necesario dotar al sistema de algunas medidas de seguridad. El emisor puede querer asegurarse de que sólo el destino deseado reciba los datos, y el receptor querrá estar seguro de que los datos recibidos no se han alterado en la transmisión y dichos datos realmente provienen del supuesto emisor.

Todo sistema de comunicaciones es complejo, por lo que debe ser diseñado cuidadosamente, ya que se necesita integrar funcionalidades de gestión de red para configurar el sistema, monitorizar su estado, reaccionar ante fallos y sobrecargas y planificar con acierto los crecimientos futuros.

Modelo de referencia OSI

En el intercambio de datos entre computadoras los procedimientos para llevarse a cabo pueden ser bastante complejos. Por este motivo se necesita un acuerdo entre los dispositivos involucrados en la comunicación para que el envío y recepción de los datos se efectúe correctamente. Por lo tanto, se necesitan un conjunto de reglas lógicas que los dispositivos deben seguir para comunicarse, a esto se le conoce como protocolo. Cuando varias computadoras y otros dispositivos de red implementan estos protocolos, especificaciones físicas y reglas, y los dispositivos están conectados correctamente las computadoras pueden comunicarse con éxito.

Los distintos fabricantes pueden hacer uso de distintos formatos y protocolos de intercambio de datos, lo que imposibilitaría la comunicación con dispositivos de otro fabricante, por lo que es necesario implementar un conjunto de convenciones comunes, llamados estándares. Así, cualquier fabricante de dispositivos tiene la

obligación de diseñar sus productos de acuerdo a estos estándares de comunicación si desea su ingreso o permanencia en el mercado, ya que el cliente puede exigir que el fabricante implemente los estándares.

Los estándares son necesarios para promover la interoperabilidad entre los equipos de distintos fabricantes. Debido a la complejidad que implican las comunicaciones, un sólo estándar no es suficiente. Se requieren un conjunto de estándares gestionados por módulos separados en partes más manejables, esto permite que el intercambio de datos se realice fiablemente, lo que constituye una arquitectura de comunicaciones.

Hay dos arquitecturas que han sido determinantes y básicas en el desarrollo de los estándares de comunicación: el conjunto de protocolos TCP/IP y el modelo de referencia OSI. TCP/IP es la arquitectura más usada, OSI nunca ha tenido éxito en el mercado, sin embargo, se utiliza como recurso explicativo de una arquitectura de protocolos.

La Organización Internacional de Estandarización (ISO, *International Organization for Standarization*) estableció el modelo de referencia OSI, basado en capas. En esta arquitectura, las funciones de comunicación se distribuyen en un conjunto jerárquico de capas. Cada capa realiza un subconjunto de tareas, relacionadas entre sí, de entre las necesarias para llegar a comunicarse con otros sistemas. Cada par se sustenta en la capa inmediatamente inferior, la cual realizará funciones más elementales, ocultando los detalles a las capas superiores. Una capa proporciona servicios a la capa inmediatamente superior. De esta forma la comunicación se descompone en varios pasos, lo que permite el monitoreo, detección y corrección de errores de manera eficiente.

La labor de ISO consistió en definir el conjunto de capas, así como los servicios a realizar por cada una de ellas. El modelo de referencia resultante tiene siete capas, cuando una aplicación X tiene un mensaje para enviar a la aplicación Y, transfiere estos datos a una entidad de la capa de aplicación. A los datos se les añade una cabecera que contiene información necesaria para el protocolo de la capa 7 (primer encapsulado). A continuación, los datos originales más la cabecera se pasan como una unidad a la capa 6. La entidad de presentación trata la unidad completa como si

de datos se tratara y le añade su propia cabecera (segundo encapsulado). Este proceso continúa hasta llegar a la capa 2, llamada trama, se pasa al medio de transmisión mediante la capa física. Cuando el dispositivo destino recibe la trama, ocurre el proceso inverso. Conforme los datos ascienden, cada capa elimina la cabecera más externa, actúa sobre la información de protocolo contenida en ella y pasa el resto de la información hacia la capa inmediatamente superior.

En cada etapa del proceso, cada una de las capas puede fragmentar la unidad de datos que recibe de la capa inmediatamente superior en varias partes. Estas unidades de datos deben ser ensambladas por la capa par correspondiente antes de pasarlas a la capa superior.

Figura 5.1 Capas del modelo OSI.

El objetivo principal que motivó el desarrollo del modelo OSI fue proporcionar un modelo de referencia para la normalización. Dentro del modelo, en cada capa se puede desarrollar uno o más protocolos. El modelo define en términos más generales las funciones que se deben realizar en cada capa y simplifica el procedimiento de la normalización.

El establecimiento de normas o estándares se puede desarrollar independiente y simultáneamente. Esto acelera el proceso de normalización, ya que las funciones de cada capa están bien definidas, los cambios que se realicen en los estándares para una capa dada no afectan al software de las otras. Esto hace que sea más fácil introducir nuevas normalizaciones.

En la comunicación entre capas, se utiliza el principio de ocultación de la información, es decir, las capas inferiores abordan ciertos detalles de tal manera que las capas superiores sean ajenas a las particularidades de estos detalles. Dentro de cada capa, se suministra el servicio proporcionado a la capa inmediatamente superior, a la vez que se implementa el protocolo con la capa par en el sistema remoto.

Arquitectura de protocolos TCP/IP

Como se mencionó en la historia de las redes de computadoras, la arquitectura de protocolos TCP/IP, es el resultado de la investigación y desarrollo llevados a cabo en la red experimental de de conmutación de paquetes ARPANET, y se denomina globalmente como la familia de protocolos TCP/IP. Esta familia consiste en una extensa colección de protocolos que se han especificado como estándares de Internet.

El modelo TCP/IP comprende cuatro capas relativamente independientes como estructura para el problema de la comunicación.

Figura 5.2 Capas del modelo TCP/IP.

Nota

Cisco utiliza el modelo TCP/IP de 4 capas. Algunos autores utilizan el moldeo TCP/IP de 5 capas, agregando la capa Física en la parte inferior de la pila. Para efectos de este proyecto ambos modelos son aceptables.

La capa física define la interfaz física ente el dispositivo de transmisión de datos y el medio de transmisión o red. Esta capa se encarga de la especificación de las características y del medio de transmisión, la naturaleza de las señales, la velocidad de los datos y cuestiones afines.

La capa de acceso a la red es responsable del intercambio de datos entre el sistema final y la red a la cual está conectado. El emisor debe proporcionar a la dirección de destino, de tal manera que ésta pueda encaminar los datos hasta el destino apropiado. El software en particular que se use en esta capa dependerá del tipo de red que se disponga, por tanto tiene sentido separar en una capa diferente todas aquellas funciones que tengan que ver con el acceso a la red. El software de las capas superiores debería, por tanto, funcionar correctamente con independencia de la red a la que el computador esté conectado.

La capa internet gestiona el acceso y encaminamiento de los datos, en situaciones en que los dispositivos estén conectados a redes diferentes, se necesitarán una serie de procedimientos que permitan que los datos atraviesen las distintas redes interconectadas. El protocolo de internet (IP, *Internet Protocol*) se utiliza en esta capa para ofrecer el servicio de encaminamiento a través de varias redes. Este protocolo se implementa tanto en los sistemas finales como en los routers intermedios.

La capa de transporte permite que los datos se intercambien de forma fiable, independientemente de la naturaleza de las aplicaciones que estén intercambiando datos. Asegura que todos los datos lleguen a la aplicación destino en el mismo orden en el que fueron enviados. Los mecanismos que proporcionan esta fiabilidad son esencialmente independientes de la naturaleza de las aplicaciones. Por tanto tiene sentido agrupar todos estos mecanismos en una capa común compartida por todas las aplicaciones. El Protocolo para el Control de la Transmisión (TCP, *Transmission Control Protocol*), es el más utilizado para proporcionar esta funcionalidad.

La capa de aplicación contiene toda la lógica necesaria para posibilitar las distintas aplicaciones de usuario, proporciona una interfaz entre el software que se está

ejecutando en una computadora y la propia red. Esta capa no define la aplicación en sí, sino los servicios que las aplicaciones necesitan.

A manera de conclusión, en la familia de protocolos TCP/IP cada capa interacciona con sus capas inmediatamente adyacentes. En el origen, la capa de aplicación utilizará los servicios de la capa extremo-a-extremo, pasándole los datos. Este procedimiento se repite en la interfaz entre la capa extremo-a-extremo y la capa internet, e igualmente en la interfaz entre la capa internet y la capa de acceso a la red. En el destino, cada capa entrega los datos a la capa superior adyacente.

La arquitectura TCP/IP no exige que se haga uso de todas las capas. Es posible desarrollar aplicaciones que invoquen directamente los servicios de cualquier capa. La mayoría de las aplicaciones requieren un protocolo extremo-a-extremo fiable y, por tanto, utilizan TCP. Otras aplicaciones de propósito específico no necesitan de los servicios del TCP.

OSI V.S. TCP/IP

El modelo de referencia OSI consta de siete capas. Cada una define un conjunto de funciones de red típicas. Cuando se estaba desarrollando OSI en las décadas de 1980 y 1990, los comités OSI crearon protocolos y especificaciones nuevas para implementar las funciones especificadas por cada capa. Así como para TCP/IP, los comités OSI no crearon nuevos protocolos o estándares, sino que hicieron referencia a otros que ya estaban definidos. Por ejemplo, el IEEE define los estándares Ethernet, por lo que los comités OSI no perdieron el tiempo especificando un nuevo tipo de Ethernet, simplemente hicieron referencia a los estándares Ethernet del IEEE.

Actualmente, el modelo OSI se puede utilizar como una norma de comparación con otros modelos de red. En la siguiente figura se compara el modelo OSI de siete capas con el modelo TCP/IP de cuatro.

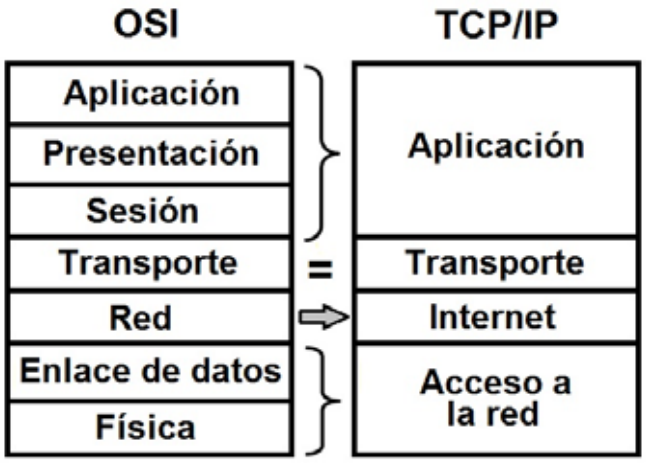


Figura 5.3 Comparación entre modelo OSI y TCP/IP.

Aunque la figura 5.3 parece implicar que la capa de red OSI y la capa Internet de TCP/IP son cuando menos similares, la figura no señala por qué son parecidas. Para apreciar por qué las capas TCP/IP se corresponden con una capa OSI en particular, se tiene que conocer ampliamente OSI. Por ejemplo, la capa de red OSI define el direccionamiento lógico y el enrutamiento, al igual que la capa Internet de TCP/IP. Aunque los detalles difieren significativamente, porque la capa de red OSI y la capa Internet de TCP/IP definen objetivos y características parecidos, la capa Internet TCP/IP equivale al a capa de red OSI. De forma parecida, la capa de transporte de TCP/IP define muchas funciones, incluyendo la recuperación ante errores, que también define la capa de transporte OSI; por esta razón, a TCP se le conoce como protocolo de la capa de transporte, o de la capa 4.

No todas las capas de TCP/IP equivalen a una sola capa OSI. En particular, la capa de acceso al a red de TCP/IP define tanto las especificaciones de la red física como los protocolos que se usan para controlar la red física. OSI separa las especificaciones de la red física en la capa física y las funciones de control en la capa de enlace de datos. De hecho, muchos piensan en TCP/IP como en un modelo de cinco capas, sustituyendo la capa de acceso a la red de TCP/IP por dos capas, una capa física y una capa de enlace de datos, para coincidir con OSI.

Nota

La explicación de la comunicación entre capas y protocolos de cada una de ellas para ambos modelos queda fuera del alcance de este proyecto.

6. Redes de Área Local (LANs)

La tendencia de las redes de área local (LAN, *Local Area Network*) implica el uso de medios de transmisión o conmutación compartidos para lograr altas velocidades de transmisión de datos en distancias relativamente cortas. Varios conceptos clave surgen por sí mismos. Uno es la elección del medio de transmisión. Mientras que el cable coaxial ha sido el medio más usado tradicionalmente, las instalaciones LAN actuales enfatizan el uso de pares trenzados de fibra óptica. En el caso de pares trenzados, se necesitan esquemas de codificación eficientes para lograr velocidades de transmisión altas a través del medio.

Una red LAN consiste en un medio de transmisión compartido y un conjunto de software y hardware para servir de interfaz entre los dispositivos y el medio. Así como para regular el acceso ordenado al mismo. Las topologías comúnmente usadas para las LAN son anillo, bus, árbol y estrella. Se han definido un conjunto de estándares LAN que especifica un rango de velocidades y comprende todas las topologías y medios de transmisión.

Mientras que las redes de área amplia o extensa pueden ser tanto públicas como privadas, las LAN son generalmente propiedad de una organización que utiliza la red para interconectar equipos. Las redes LAN tienen mucha mayor capacidad que las de área amplia, permitiendo el transporte de un tráfico interno generalmente superior.

Una configuración común de red LAN es aquella que consta de computadoras personales. Dado el costo relativamente bajo de estos sistemas, algunos administradores de organizaciones adquieren frecuentemente computadoras personales para aplicaciones departamentales, como hojas de cálculo y herramientas de gestión de proyectos, además del acceso a Internet. Sin embargo, una red de este tipo de computadoras no cubre todas las necesidades de un organismo, también son necesarios servicios de procesamiento central. Algunas aplicaciones son demasiado grandes para poder ejecutarse en una PC. Los archivos de datos corporativos de gran tamaño, como los correspondientes a contabilidad y nóminas, precisan de un servicio centralizado al tiempo que deberían ser accesibles por parte de distintos usuarios. Además, hay otros tipos de archivos,

aunque especializados, deben compartirse entre diferentes usuarios. Existen también razones de peso para llevar a cabo la conexión de estaciones de trabajo inteligentes individuales no sólo a un servicio central, sino también entre sí. Los miembros del equipo de un proyecto o de un organismo necesitan compartir trabajo e información, siendo la forma digital la más eficiente para hacerlo.

Otro tipo de recursos de costo elevado, como una multifuncional, pueden ser compartidos por todos los usuarios de una LAN departamental. Además, la red puede servir de nexo entre servicios de red corporativos mayores. Por ejemplo, la compañía puede disponer de una LAN a nivel de edificio y de una red privada de área amplia. Un servidor de comunicaciones puede proporcionar acceso controlado a estos recursos.

La utilización de redes LAN para dar soporte a computadoras personales y estaciones de trabajo se ha convertido en un hecho casi universal en todo tipo de organizaciones. Gracias a estas redes, las corporaciones pueden gestionar de manera óptima sus recursos y mejorar la productividad en sus diferentes áreas, además de mejorar el servicio al cliente.

6.1 Características y componentes de las LANs

Medios de Transmisión

En un sistema de intercambio de datos, el medio de trasmisión es el camino físico entre el transmisor y el receptor. Las ondas electromagnéticas se transmiten a través de un medio sólido, como por ejemplo, un par trenzado de cobre, un cable coaxial o una fibra óptica. En los medios no guiados, la transmisión inalámbrica se realiza a través de la atmósfera, el espacio exterior o el agua.

Las características y calidad de la transmisión están determinadas tanto por el tipo de señal como por las características del medio. En el caso de los medios guiados, el medio, en sí mismo es lo que más limitaciones impone a la transmisión.

En medios no guiados, las características de la transmisión están más determinadas por el ancho de banda de la señal emitida por la antena que por el propio medio. Una propiedad fundamental de las señales transmitidas mediante antenas es la direccionalidad. En general, a frecuencias bajas las señales son omnidireccionales; es decir, la señal desde la antena se emite y propaga en todas direcciones. A frecuencias más altas, es posible concentrar la señal en un haz direccional.

En el diseño de los sistemas de transmisión es deseable que tanto la distancia como la velocidad de transmisión sean lo más grandes posibles. Hay una serie de factores relacionados con el medio de transmisión y con la señal que determinan tanto la distancia como la velocidad de transmisión:

- **Ancho de Banda**: si todos los otros factores se mantienen constantes, al aumentar el ancho de banda de la señal, la velocidad de transmisión se puede incrementar.
- **Dificultades en la transmisión**: las dificultades, como por ejemplo la atenuación, limitan la distancia. En los medios guiados, el par trenzado sufre de mayores adversidades que el cable coaxial que, a su vez, es más vulnerable que la fibra óptica.
- **Interferencias**: las interferencias resultantes de la presencia de señales en bandas de frecuencia próximas pueden distorsionar o destruir la señal. Las interferencias son especialmente relevantes en los medios no guiados, pero a la vez son un problema a considerar en los medios guiados, las emisiones de cables cercanos pueden causar interferencias. Así por ejemplo, es frecuente embutir múltiples cables de pares trenzados dentro de una misma cubierta. Las interferencias también pueden aparecer en las transmisiones no guiadas. Un blindaje adecuado del medio guiado puede minimizar este problema.
- **Número de receptores**: un medio guiado se puede usar tanto para un enlace punto a punto como para un enlace compartido, mediante el uso de múltiples conectores. En este último caso, cada uno de los conectores utilizados puede atenuar y distorsionar la señal, por lo que la distancia y/o la velocidad de transmisión disminuirán.

Medios de transmisión guiados

En los medios de transmisión guiados, la capacidad de transmisión, en términos de velocidad de transmisión o ancho de banda, depende drásticamente de la distancia y de si el medio es punto a punto o multipunto. Los medios guiados más utilizados en la transmisión de datos son el par trenzado, el cable coaxial y la fibra óptica.

Par trenzado

Consiste en dos cables de cobre embutidos en un aislante entrecruzados en forma de bucle espirar. Cada par de cables constituye un enlace de comunicación. Normalmente, varios pares se encapsulan conjuntamente mediante una envoltura protectora. En el caso de largas distancias, la envoltura puede contener cientos de pares. El uso del trenzado tiende a reducir las interferencias electromagnéticas (diafonía) entre los pares adyacentes dentro de una misma envoltura. Para este fin, los pares adyacentes dentro de una misma envoltura se trenzan con pasos de torsión diferentes. En enlaces de larga distancia, la longitud del tranzado varía entre 5 cm y 15 cm. Los conductores que forman el par tienen un grosor que varía entre 0.4 mm y 0.9 mm.

El par trenzado es el medio más usado en las redes de telefonía e, igualmente, su uso es básico en el tendido de redes de comunicación dentro de edificios, por su bajo costo y facilidad de manejo.

Par trenzado blindado y sin blindar

Hay dos variantes de pares trenzados: blindados y no blindados. En telefonía, el par trenzado no blindado (UTP, *Unshielded Twisted Pair*) es el cable más habitual. En edificios es común la preinstalación de par trenzado no blindado, aunque normalmente se dimensiona muy por encima de lo que verdaderamente se necesita para el servicio de telefonía. Esto es así porque el par sin blindar es el menos caro

de todos los medios de transmisión que se usan en las redes de área local, además de ser fácil de instalar y manipular.

El par trenzado sin blindaje se puede ver afectado por interferencias electromagnéticas externas, incluyendo interferencias de pares cercanos o fuentes de ruido próximas, una manera de mejorar las características de transmisión de este medio es protegiéndolo dentro de una malla metálica, reduciéndose así las interferencias. El par trenzado blindado (STP, *Shield Twisted Pair*) proporciona mejor rendimiento a velocidades de transmisión superiores. Ahora bien, este último es más costoso y difícil de manipular que el anterior.

Categorías UTP

En la mayoría de los edificios corporativos construidos en la segunda mitad de los noventa, se preinstalaba cable UTP categoría 3 (*voice-grade*), era una alternativa bastante atractiva y poco costosa para ser utilizada como medio de transmisión en las LAN, sin embargo, las velocidades de transmisión que se pueden alcanzar con este medio son limitadas.

En 1991, la Asociación de Industrias Electrónicas (EIA, *Electronic Industries Association*) publicó el documento EIA-568, denominado Estándar para los Cables de Telecomunicaciones en Edificaciones Comerciales (*Commercial Building Telecommunications Cabling Standard*), que define el uso de pares trenzados no blindados de calidad telefónica y de pares blindados como medios de transmisión de datos en edificios. Cabe mencionar, que en aquel tiempo, las características de dichos medios eran suficientes para el rango de frecuencias y velocidades típicas necesarias en las aplicaciones ofimáticas. Es más, en esa época las LAN tenían como objetivo velocidades de transmisión comprendidas entre 1 y 16 Mbps. Con el tiempo, los usuarios han migrado a estaciones de trabajo y aplicaciones de mayores requerimientos. Como consecuencia, hubo un interés creciente en LAN que proporcionaran hasta 100 Mbps sobe medios no costosos.

Como respuesta a esta necesidad, en 1995 se propuso el EIA-568-A. Esta norma incorpora avances más recientes, tanto en el diseño de cables y conectores, como en los métodos de test.

Las aplicaciones que corrían sobre las redes, fueron creciendo y demandando mayores recursos y como consecuencia, ancho de banda. Con la creación de la norma EIA-568-A, a partir de 1995 se comenzó a preinstalar en edificios de oficinas cable UTP de categoría 5 (data-grade) que posee mejores características para la transmisión de datos, por lo que es común hoy en día encontrar este tipo de cableado en la mayoría de las construcciones relativamente recientes. Con un diseño apropiado y a distancias limitadas, con cables categoría 5 se pueden alcanzar velocidades de 100 Mbps.

A continuación se muestran las características principales de cada categoría de cable UTP:

- **Categoría 1**: Hilo telefónico trenzado de calidad de voz no adecuado para las transmisiones de datos. Las características de transmisión del medio están especificadas hasta una frecuencia superior a 1MHz.
- **Categoría 2**: Cable par trenzado sin blindar. Las características de transmisión del medio están especificadas hasta una frecuencia superior de 4 MHz. Este cable consta de 4 pares trenzados de hilo de cobre.
- **Categoría 3**: Velocidad de transmisión típica de 10 Mbps para Ethernet. Con este tipo de cables se implementan las redes Ethernet 10BaseT. Las características de transmisión del medio están especificadas hasta una frecuencia superior de 16 MHz. Este cable consta de cuatro pares trenzados de hilo de cobre con tres entrelazados por pie.
- **Categoría 4**: La velocidad de transmisión llega hasta 20 Mbps. Las características de transmisión del medio están especificadas hasta una frecuencia superior a 20 MHz. Este cable consta de 4 pares trenzados de hilo de cobre.
- **Categoría 5**: Es una mejora de la categoría 4, puede transmitir datos hasta 100Mbps y las características de transmisión del medio están especificadas hasta una frecuencia superior de 100 MHz. Este cable consta de cuatro pares trenzados de hilo de cobre.

- **Categoría 6**: Es una mejora de la categoría anterior, puede transmitir datos hasta 1Gbps y las características de transmisión del medio están especificadas hasta una frecuencia superior a 250 MHz.
- **Categoría 7**. Es una mejora de la categoría 6, puede transmitir datos hasta 10 Gbps y las características de transmisión del medio están especificadas hasta una frecuencia superior a 600 Mhz.

En la actualidad, la demanda de ancho de banda para aplicaciones empresariales es enorme, además con la introducción de las redes sociales y los portales web multiservicios, muchas empresas han tenido que optar por medios de transmisión de mejor rendimiento, como es la fibra óptica, cuyas características salen de este estudio.

7. Ethernet

Ethernet ha sido la tecnología LAN de mayor éxito, en gran medida, debido a la simplicidad de su implementación, cuando se le compara con otras tecnologías. Ethernet también ha tenido éxito porque es una tecnología flexible que ha evolucionado para satisfacer las cambiantes necesidades y capacidades de los medios.

El término Ethernet se refiere a una familia de estándares que en conjunto definen la capa física y la capa de enlace de datos del tipo de LAN más popular del mundo. Los diferentes estándares varían en lo que se refiere a la velocidad soportada, con velocidades de 10/100/1000 Mbps. Los estándares también difieren en cuanto a los tipos de cableado y longitud permitida para el cableado. Los estándares Ethernet más comúnmente utilizados permiten el uso de cableado UTP barato, mientras que otros estándares exigen un cableado de fibra óptica, más caro. El costo del cableado de fibra óptica podría merecer la pena en algunos casos porque resulta más seguro y permite distancias mucho mayores entre dispositivos. A fin de soportar necesidades tan diversas en cuanto a la construcción de una LAN (diferentes velocidades, diferentes tipos de cableado, comparando requisitos de distancia y costo, etc.) y otros factores, se han creado muchos estándares Ethernet.

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, *Institute of Electrical and Electronic Engineers*) ha definido muchos estándares Ethernet desde que inició el proceso de estandarización de las LANs a principios de la década de 1980. La mayoría de los estándares definen una variación diferente de Ethernet en la capa física, con diferencias en cuanto a velocidad y tipos de cableado. Además para la capa de enlace de datos, el IEEE separa las funciones en dos subcapas:

- Subcapa 802.3 MAC (Control de acceso al medio, *Media Access Control*).
- Subcapa 802.2 LLC (Control de enlace lógico, *Logical Link Control*).

De hecho las direcciones MAC toman su nombre del nombre IEEE para esta porción inferior de los estándares Ethernet de la capa de enlace de datos.

Cada nuevo estándar de la IEEE para la capa física requiere muchas diferencias en esta capa. Sin embargo, cada uno de estos estándares de la capa física utiliza exactamente la misma cabecera 802.3, y cada uno también usa la subcapa LLC superior. A continuación se muestran los estándares de la capa física Ethernet del IEEE que más se utilizan:

Nombre común	Velocidad	Nombre alternativo	Nombre del estándar IEEE	Tipo de Cable, longitud máxima
Ethernet	10 Mbps	10BASE-T	IEEE 802.3	Cobre, 100 m.
Fast Ethernet	100 Mbps	100BASE-TX	IEEE 802.3u	Cobre, 100 m.
Gigabit Ethernet	1000 Mbps	1000BASE-LX 1000BASE-SX	IEEE 802.3z	Fibra, 550 m. (SX) Fibra, 5 km. (LX)
Gigabit Ethernet	1000 Mbps	1000BASE-T	IEEE 802.3ab	Cobre, 100m

Tabla 7.1 Estándares IEEE más comunes.

Conectores RJ-45 en cables UTP

El cableado UTP utilizado por los estándares Ethernet incluye dos o cuatro pares de hilos. Como los hilos que hay dentro de un cable son delgados y frágiles, el propio cable tiene una cubierta exterior de plástico flexible para dar consistencia a los hilos. Cada hilo de cobre individual tiene un fino recubrimiento de plástico que ayuda a evitar sus roturas. El revestimiento plástico de cada hilo tiene un color diferente para que sea más fácil observar los extremos del cable e identificar los extremos de un hilo específico. El cable termina con algún tipo de conector (normalmente, conectores RJ-45), con los extremos de los hilos insertados en los pines. El conector RJ-45 tiene ocho lugares físicos específicos en los que pueden insertarse los ocho hilos del cable, denominados posiciones de los pines o simplemente pines. Para instalar conectores al final del cable, los extremos de los hilos deben estar correctamente insertados en las posiciones de pines correctas. Una vez que se tiene el cable con sus conectores RJ-45 en los extremos, se puede conectar a un puerto Ethernet de la tarjeta de red, switch o router.

Transmisión de datos usando UTP

Cuando se tienen dos dispositivos conectados entre sí por un cable UTP, se está listo para la transmisión. Los dispositivos de cada extremo del cable pueden crear un circuito eléctrico al enviar corriente por un par de hilos, en direcciones opuestas. Cuando la corriente pasa por cualquier hilo, esa corriente induce un campo magnético hacia el exterior del hilo; el trenzar juntos los hilos de un mismo par, con la corriente circulando en direcciones opuestas por cada hilo, el campo magnético creado por un hilo cancela en su mayor parte el campo magnético creado por el otro hilo. Debido a esta característica, la mayoría de los cables de red que usan hilos de cobre y electricidad recurren a pares de hilos trenzados para enviar los datos.

Para enviar datos por el circuito eléctrico creado sobre un par de hilos, los dispositivos utilizan un esquema de codificación que define como debe variar, con el transcurso del tiempo, la señal eléctrica para denotar un 1 o un 0 binario. Los detalles de codificación están fuera del alcance de este proyecto, sin embargo, es importante mencionar que los dispositivos de red crean un circuito eléctrico utilizando cada par de hilos, y la señal varía según lo define el esquema de codificación, para enviar los bits por el par de hilos.

Los hilos de un cable UTP deben estar conectados en las posiciones de pin adecuadas de los conectores RJ-45 para que la comunicación sea correcta. El conector RJ-45 tiene 8 posiciones de pin, o simplemente pines, en lo que destacan los ocho hilos de cobre del cable. La elección de qué color va en cada posición se basa en los estándares creados por la Asociación en la Industria de las Telecomunicaciones (TIA, *Telecommunications Industry Association*) y la Asociación de Industrias Eléctricas (EIA, *Electronics Industry Alliance*), las cuales definen los estándares oficiales para la fabricación del cableado UTP, la codificación por colores de los cables y los *pinouts* estándar en los cables.

Para construir una LAN Ethernet que funcione, se deben elegir cables que utilicen el *pinout* de cableado correcto en cada extremo del cable. Existen dos tipos de cables, el recto y el cruzado. Para crear un cable recto, los dos extremos del cable obedecen el mismo *pinout* EIA/TIA estándar. Por ejemplo, en un cable recto se conecta el hilo del pin 1 de un extremo del cable con el pin 1 del otro extremo del

cable; el hilo del pin 2 tiene que conectar con el pin 2 del otro extremo; el pin 3 de un extremo está conectado al pin 3 del otro, y así sucesivamente.

Un cable recto se utiliza cuando los dispositivos conectados a los extremos del cable utilizan pines opuestos cuando transmiten datos. No obstante, al conectar dos dispositivos que utilizan los mismos pines para transmitir. Los *pinouts* del cable deben configurarse para intercambiar los pares de hilos. Un cable que intercambia los pares de hilos dentro del cable recibe el nombre de cable cruzado.

CSMA/CD

Cuando dos tramas colisionan, el medio permanece inutilizable mientras dura la transmisión de ambas tramas dañadas. En el caso de que la longitud de las tramas sea elevada en comparación con el tiempo de propagación, la cantidad de tiempo desaprovechado puede ser considerable. Este desaprovechamiento de la capacidad puede reducirse si una estación continúa escuchando el medio mientras dura la transmisión. La lógica CSMA/CD (Acceso Múltiple por Detección de Portadora con Detección de Colisiones, *Carrier Sense Multiple Access with Collision Detection*) ayuda a evitar las colisiones y define cómo actuar cuando se produce una colisión.

CSMA/CD opera de la siguiente manera:

1. Un dispositivo con una trama por enviar, escucha hasta que Ethernet deja de estar ocupado.
2. Cuando Ethernet no está ocupado, el(los) emisor(es) empieza(n) a enviar la trama.
3. El(los) emisor(es) escucha(n) para asegurarse de que no se ha producido una colisión.
4. Si se produce una colisión, los dispositivos que estuvieran enviando una trama enviarán cada uno una señal de interferencia para asegurase de que todas las estaciones reconocen la colisión.

5. Una vez completada la interferencia, cada emisor pone a funcionar aleatoriamente un temporizador y espera algún tiempo antes de intentar enviar la trama que colisionó.
6. Cuando expira el temporizador aleatorio, el proceso empieza de nuevo con el paso 1.

Protocolos de enlace de datos Ethernet

Uno de los aspectos más significativos de la familia de protocolos de Ethernet es que estos protocolos utilizan el mismo pequeño conjunto de estándares de enlace de datos. Por ejemplo, el direccionamiento de Ethernet funciona de la misma forma en todas las variantes de Ethernet, incluyendo los estándares de Ethernet que usan otros tipos de cableado aparte de UTP. Además el algoritmo CSMA/CD es técnicamente una aparte de la capa de enlace de datos, aplicable de nuevo a la mayoría de tipos de Ethernet, a menos que se haya desactivado.

Direccionamiento de Ethernet

El direccionamiento de una LAN Ethernet identifica los dispositivos individuales o grupos de dispositivos que hay en una LAN. Una dirección tiene 6 bytes de longitud, está escrita normalmente en hexadecimal y en algunos dispositivos con puntos separando los conjuntos de cuatro dígitos hexadecimales.

En la unidifusión, una dirección Ethernet identifica un tarjeta LAN en concreto. Las computadoras utilizan direcciones de unidifusión para identificar el emisor y el receptor de una trama Ethernet.

El IEEE define el formato y la asignación de las direcciones de LAN. El IEEE requiere direcciones MAC globalmente únicas en todas las tarjetas de interfaz de LAN. Para garantizar una dirección única, los fabricantes de tarjetas Ethernet codifican la dirección MAC en la tarjeta, normalmente en un chip ROM. La primera mitad en la dirección identifica al fabricante de la tarjeta. Este código, que el IEEE

asigna a cada fabricante, se denomina identificador único de organización (OUI, *Organizationally Unique Identifier*). Cada fabricante asigna un número OUI propio como primera mitad de la dirección, y la segunda mitad le asigna un número que nunca ha utilizado en otra tarjeta.

Se pueden utilizar muchos términos para describir las direcciones LAN de unidifusión. Cada tarjeta LAN viene con una dirección física (integrada o prefijada) (BIA, *Burned-In Address*) que se "quema" en el chip ROM de la tarjeta. Las BIAs reciben a veces el nombre de direcciones universalmente administradas (UAA, *Universally Administered Addresses*) porque el IEEE administra globalmente la asignación de direcciones. Independientemente de si se utiliza la BIA o se configura otra dirección, muchos se refieren a las direcciones de unidifusión como direcciones LAN, direcciones de Ethernet, direcciones de hardware, direcciones físicas o direcciones MAC.

A continuación se muestran los diferentes grupos de direcciones:

- **Direcciones de grupo.** Identifican más de una tarjeta de interfaz LAN. El IEEE define dos categorías generales de direcciones de grupo para Ethernet.
- **Direcciones de difusión**: Son las más utilizadas del grupo de direcciones MAC del IEEE. Tiene un valor de FFFF.FFFF.FFFF (notación hexadecimal). La dirección de difusión implica que todos los dispositivos de la LAN deben procesar la trama.
- **Direcciones de multidifusión**. Las direcciones de multidifusión se utilizan para que un subconjunto de dispositivos de una LAN puedan comunicarse. Cuando IP multidifunde por una Ethernet, las direcciones MAC de multidifusión utilizadas por IP respetan este formato: 0100:5exx.xxxx, donde pude utilizarse cualquier valor en la última mitad de la dirección.

Entramado Ethernet

El entramado define cómo se interpreta una cadena de números binarios. Es decir, el entramado define el significado que hay detrás de los bits que se transmiten a través de una red. La capa física ayuda a obtener una cadena de bits de un dispositivo a otro. El término entramado se refiere a la definición de los campos que se asume que están en los datos recibidos. Es decir, el entramado define el significado de los bits transmitidos y recibidos por una red.

El entramado usado para Ethernet ha cambiado un par de veces a lo largo de los años. Xerox definió una versión del entramado, que el IEEE modificó después cuando se encargó de los estándares de Ethernet a principios de la década de 1980. El IEEE finalizó un compromiso estándar para el entramado en 1997 que incluía algunas de las características del entramado Ethernet original de Xerox, junto con el entramado definido por el IEEE. El resultado final es el formato de trama siguiente:

	Preámbulo	**SFD**	**Destino**	**Origen**	**Longitud**	**Datos y relleno**	**FCS**
Bytes	7	1	6	6	2	46 – 1500	4

Figura 7.1 Formato de la cabecera IEEE 802.3.

Identificación de los datos de una trama Ethernet

A lo largo de los años se han diseñado muchos protocolos de capa de red (capa 3) diferentes. La mayoría de estos protocolos eran parte de modelos de protocolo de red más grandes creados por los fabricantes con el objetivo de que se pudieran soportar sus productos, como SNA (Arquitectura de sistemas de red, *Systems Network Architecture*) de IBM, Novell NetWare, DECnet de *Digital Equimpmet Corporation* y AppleTalk de Apple Computer. Además, los modelos OSI y TCP/IP también definieron protocolos de capa de red.

Todos estos protocolos de la capa 3, más algunos otros, podían utilizar Ethernet. Para ello, el protocolo de la capa de red debía colocar su paquete (L3 PDU) en la porción de datos de la trama Ethernet mostrada en la figura 7.1. Sin embargo,

cuando un dispositivo recibe una trama Ethernet de este tipo, dicho dispositivo receptor necesita conocer el tipo de L3 PDU que hay en la trama Ethernet e identificar si se trata de un paquete IP, un paquete OSI o SNA, etc.

Para responder a esta cuestión, las cabeceras de la mayoría de los protocolos de enlace de datos, incluyendo Ethernet, tienen un campo con un código de define el tipo de cabecera de protocolo que va a continuación. En términos generales estos campos en las cabeceras de enlace de datos se denominan “campos de tipo”. Es interesante observar que, debido a los cambios introducidos en el entramado Ethernet a lo largo de los años, existe otra popular opción para el campo tipo de un protocolo, particularmente cuando se envían paquete IP.

Detección de errores

La última función de la capa de enlace de datos de Ethernet es la detección de errores. Se trata de un proceso de descubrir si los bits de una trama han cambiado como resultado de su envío por la red. Los bits podrían cambiar por muchas razones, pero generalmente dichos errores se producen como resultado de alguna clase de interferencia eléctrica. Para evitar errores en la transmisión, Ethernet define una cabecera y una información final, esta última contiene un campo que se utiliza con el objetivo de detectar errores.

El capo Secuencia de Verificación de Trama (FCS, *Frame Check Sequence*) en la información final de Ethernet permite a un dispositivo que recibe una trama Ethernet detectar si los bits han cambiado durante la transmisión. Para detectar un error, el dispositivo emisor calcula una función matemática compleja, con el contenido de la trama como entrada, colocando el resultado en el campo FCS de 4 bytes de la trama. El dispositivo receptor hace el mismo cálculo en la trama; si el resultado del cálculo no coincide, se ha producido un error y la trama es descartada. Esta detección de errores tampoco significa una recuperación ante errores. Ethernet define que la trama errónea debe descartarse, pero no hace nada para que la trama sea retransmitida. Otros protocolos, en especial TCP pueden repara en la pérdida de datos y forzar una recuperación ante los errores.

8. Direccionamiento y enrutamiento IP

Los protocolos equivalentes a la capa 3 de OSI definen la entrega de los paquetes desde la computadora que crea el paquete hasta llegar a la computadora que debe recibir el paquete. Para alcanzar este objetivo, un protocolo de la capa de red OSI define las siguientes características:

- **Enrutamiento**: Es el proceso de enviar paquetes (Protocolo de Unidades de Datos (PDUs, *Protocol Data Units*) capa 3).
- **Direccionamiento lógico**: Direcciones que se pueden utilizar independientemente del tipo de red física usada, proporcionando a cada dispositivo (al menos) una dirección. Gracias al direccionamiento lógico, el proceso de enrutamiento puede identificar el origen y el destino de un paquete.
- **Protocolo de enrutamiento**: Un protocolo que ayuda a los routers a aprender dinámicamente sobre los grupos de direcciones de la red, que a la vez permite que el proceso de enrutamiento (envío) funcione correctamente.
- **Otras utilidades**: La capa de red también se apoya en otras utilidades. Para TCP/IP, estas utilidades incluyen el Sistema de Denominación de Dominio (DNS, *Domain Name System*), el Protocolo de Configuración Dinámica del Host (DHCP, *Dymanic Host Configuration Protocol*), el Protocolo de Resolución de Direcciones (ARP, *Address Resolution Protocol*), y el ping.

Funciones de la capa de red

Se considera que un protocolo que define el enrutamiento y el direccionamiento lógico es un protocolo de la capa de red o capa 3. OSI define un único protocolo de capa 3 denominado Servicios de Red sin Conexiones (CLNS, *Connectionless Network Services*), sin embargo, como es habitual con los protocolos OSI, raramente se observa en las redes actuales. En el pasado reciente era común encontrar otros protocolos de la capa de red, como Protocolo de Internet (IP, *Internet Protocol*), Intercambio de paquetes entre redes (IPX, *Internetwork Packet Exchange*), de Novell o Protocolo de entrega de datagramas (DDP, *Datagram*

Delivery Protocol) de AppleTalk. Actualmente, el único protocolo de la capa 3 que se utiliza ampliamente es el protocolo de capa de red TCP/IP; concretamente, IP.

La tarea principal de IP es enrutar los datos (paquetes) desde el host de origen hasta el host destino. Como una red podría necesitar enviar una gran cantidad de paquetes, el proceso de enrutamiento IP es muy simple. IP no requiere la sobrecarga de ningún tipo de acuerdo o mensaje antes de enviar un paquete, lo que hace de IP un protocolo "no orientado a la conexión". IP intenta entregar cada paquete, pero si el proceso IP del router o del host no puede entregarlo, es descartado, sin ningún tipo de recuperación ante errores. El objetivo con IP es entregar paquetes con el menor trabajo por paquete posible, lo que permite grandes volúmenes de paquetes. Otros protocolos llevan a cabo otras funciones de *networking* útiles. Por ejemplo, el Protocolo para el Control de la Transmisión (TCP, *Transmission Control Protocol*), ofrece la recuperación ante errores y el reenvío de los datos perdidos, pero no así IP.

Enrutamiento

El enrutamiento se centra en la lógica de extremo a extremo del envío de datos. Cuando el protocolo de capa de red está procesando el paquete, decide mandarlo a la interfaz de red apropiada. Antes de que los bits reales puedan colocarse en esa interfaz física, la capa de red debe pasar el paquete a los protocolos de capa de enlace de datos que, a su vez, solicitan a la capa física que envíe realmente los datos. La capa de enlace de datos añade la cabecera y la información final apropiadas al paquete, creando una trama, antes de enviar las tramas por cada red física. El proceso de enrutamiento envía el paquete y sólo, de extremo a extremo a través de la red, descartando por el camino las cabeceras y las informaciones finales de enlace de datos. Los procesos de capa de red entregan el paquete de extremo a extremo, utilizando cabeceras e informaciones finales sucesivas sólo para entregar el paquete al siguiente router o host de la ruta. Cada capa de enlace de datos sucesiva lleva el paquete de un dispositivo al siguiente.

Como los routers generan cabeceras e informaciones finales de enlace de datos nuevas, y como las cabeceras nuevas contienen las direcciones de enlace de datos, los PCs y los routers deben tener alguna forma de decidir qué direcciones de enlace de datos usar. Un ejemplo de cómo un router determina qué direcciones de enlace de datos usar es el Protocolo de Resolución de Direcciones (ARP, *Address Resolution Protocol*). ARP se utiliza para aprender dinámicamente la dirección de enlace de datos de un host IP conectado a una LAN.

El enrutamiento tiene dos conceptos principales:

- El proceso de enrutamiento envía paquetes de capa 3, también denominados Unidades de Datos del Protocolo de Capa 3 (*Layer 3 Protocol data Units*, o L3 PDU), basándose en la dirección de capa 3 de destino que hay en el paquete.
- El proceso de enrutamiento utiliza la capa de enlace de datos para encapsular los paquetes de capa 3 en tramas de capa 2 para su transmisión a través de cada enlace de datos sucesivo.

Paquetes IP y la cabecera IP

Los paquetes IP encapsulados en las tramas de enlace de datos, tienen una cabecera IP, seguida por cabeceras y datos adicionales. La siguiente figura muestra los campos de la cabecera IPv4 de 20 bytes estándar, sin campos de cabecera IP opcionales, como normalmente se ve en la mayoría de las redes actuales.

A continuación se describen todos los campos de la cabecera IPv4:

Campo	Significado
Versión	Versión del protocolo IP. La mayoría de las redes utilizan actualmente la versión 4, sin embargo, ya se encuentra en proceso la migración a la versión 6.
IHL	Longitud de cabecera IP. Define la longitud de la cabecera IP, incluyendo los campos opcionales.
Campo DS	Campo de servicios diferenciados. Se utiliza para marcar paquetes con el propósito de aplicar diferentes niveles de calidad de servicio (QoS, *Quality-of-Service*) a paquetes distintos.
Longitud de paquete	Identifica la longitud total del paquete IP, incluyendo los datos.
Identificación	La utiliza el proceso de fragmentación de paquetes IP; todos los fragmentos del paquete original contienen el mismo identificador.
Indicadores	3 bits que son utilizados por el proceso de fragmentación de paquetes IP.
Desplazamiento de fragmento	Es un número que se utiliza para ayudar a los hosts a reensamblar los paquetes fragmentados en el paquete original, que es más grande.
TTL	Tiempo de existencia (*Time To Live*). Es un valor que se utiliza para evitar los bucles de enrutamiento.
Protocolo	Es un campo que identifica el contenido de la porción de datos del paquete IP. Por ejemplo, protocolo 6 implica que una cabecera TCP es la primera cosa del campo de datos del paquete IP.
Suma de comprobación de la cabecera	Es un valor que se utiliza para almacenar un valor FCS (*Frame Check Sequence*). Cuyo propósito es determinar si se han producido errores en los bits de la cabecera IP.
Dirección IP de origen	Dirección IP de 32 bits del emisor del paquete.
Dirección IP de destino	Dirección IP de 32 bits del receptor pretendido del paquete.

Tabla 8.1 Campos de la cabecera IPv4.

Direccionamiento de capa de red

Los protocolos de capa de red definen el formato y el significado de las direcciones lógicas. Toda computadora que necesite comunicarse tendrá (al menos) una dirección de capa de red para que las demás computadoras puedan enviar paquetes de datos a esa dirección, esperando que la red entregue el paquete de datos a la computadora correcta.

Una característica clave de las direcciones de capa de red es que fueron diseñadas para permitir el agrupamiento lógico de las direcciones. Es decir, algo sobre el valor numérico de una dirección implica un grupo o conjunto de direcciones, considerándose que todas ellas están en el mismo agrupamiento. Con las direcciones IP, este grupo se denomina red o subred. Estos agrupamientos funcionan como los códigos postales, ya que permiten a los routers (clasificadores postales) enrutar (clasificar) rápidamente montones de paquetes (cartas).

Al igual que las direcciones postales, las direcciones de capa de red se agrupan con base en la ubicación física en una red. Las reglas difieren para algunos protocolos de capa de red, sin embargo, con el direccionamiento IP, la primera parte de la dirección IP es la misma para todas las direcciones de un grupo.

El enrutamiento se apoya en el hecho de que las direcciones de capa 3 están agrupadas. Las tablas de enrutamiento para cada protocolo de capa de red pueden tener una entrada para el grupo, no una entrada para cada una de las direcciones. Supongamos una Ethernet con 100 hosts TCP/IP. Un router que tiene que enviar paquetes a cualquiera de los otros hosts sólo necesita una entrada en su tabla de enrutamiento IP; dicha entrada de la tabla de enrutamiento representa el grupo entero de hosts de la Ethernet. Este hecho básico es una de las principales razones de que los routers puedan escalar y permitan cientos de miles de dispositivos.

Protocolos de enrutamiento

Los routers conocen de algún modo los pasos correctos a dar para enviar el paquete de una computadora a otra. Para tomar las decisiones correctas, cada router necesita una tabla de enrutamiento, con una ruta equivalente al paquete enviado a la otra computadora. Las rutas indican al router el lugar al que enviar el paquete a continuación.

En la mayoría de los casos, los routers utilizan un protocolo de enrutamiento para generar dinámicamente sus entradas de tabla de enrutamiento. Los protocolos de enrutamiento aprenden sobre todas las ubicaciones de los “grupos” de capa de red de una red y publican dichas ubicaciones. En consecuencia, cada router puede generar dinámicamente una adecuada tabla de enrutamiento. Los protocolos de enrutamiento definen los formatos de mensaje y los procedimientos, al igual que cualquier otro protocolo. El objetivo final de cada protocolo de enrutamiento es rellenar la tabla de enrutamiento con todos los grupos de destino conocidos y con la mejor ruta para alcanzar cada grupo.

La terminología relacionada con los protocolos de enrutamiento puede aprenderse sobre la marcha. Un protocolo de enrutamiento aprende rutas y las coloca en una tabla de enrutamiento. Un protocolo enrutado define el tipo de paquete enviado, o enrutado, a través de una red. IP es un protocolo enrutado. Si los routers utilizaran el Protocolo de Información de Ruteo (RIP, *Routing Information Protocol*) sería el protocolo de enrutamiento.

Direccionamiento IP

Si un dispositivo quiere comunicarse usando TCP/IP, necesita una dirección IP. Cuando el dispositivo tiene una dirección IP y el software y el hardware apropiados, puede enviar y recibir paquetes IP. Cualquier dispositivo que pueda enviar o recibir paquetes IP es un host IP.

Las direcciones IP consisten en un número de 32 bits, y normalmente se escriben en notación con punto. La parte “decimal” del término viene del hecho de que cada

byte (8 bits) de la dirección IP de 32 bits se muestra como su equivalente decimal. Los cuatros números decimales resultantes se escriben en secuencia, separados mediante “puntos”; de todo esto se deriva la expresión decimal con puntos. Por ejemplo, 168.1.1.1 es una dirección IP escrita en formato decimal con puntos; la versión binaria real es 10101000 00000001 00000001 00000001.

Cada interfaz de red utiliza una dirección IP única. La mayoría tiende a pensar que su computadora tiene una dirección IP, pero en realidad es la tarjeta de red de la computadora la que tiene una dirección IP. Si instala dos tarjetas Ethernet en una PC para enviar paquetes IP a través de las dos tarjetas, las dos necesitan direcciones IP únicas. Algunas computadoras portátiles tienen tarjeta de red inalámbrica y alámbrica, por lo tanto tienen una dirección IP para cada Tarjeta de Interfaz de Red (NIC, *Network Interface Card*). De forma parecida, los routers, que normalmente tienen muchas interfaces de red que envían paquetes IP, tienen una dirección IP para cada interfaz.

Agrupación de direcciones IP

Las especificaciones para las direcciones IP agrupadas de TCP/IP en conjuntos de direcciones consecutivas se denominan redes IP. Las direcciones de una red tienen el mismo valor numérico en la primera parte de todas las direcciones de red. Las convenciones del direccionamiento IP y del agrupamiento de direcciones IP hacen que el enrutamiento sea sencillo. Los routers crean una tabla de enrutamiento para cada entrada, una para cada prefijo, o número de red. Hay dos puntos clave sobre cómo se organizan las direcciones IP:

- Todas las direcciones IP del mismo grupo no deben estar separadas por un router.
- Las direcciones IP separadas por un router deben estar en grupos diferentes.

Por lo tanto, el enrutamiento IP se apoya en el hecho de que todas las direcciones IP del mismo grupo (denominado red o subred) se encuentran en la misma ubicación general. Si algunas de las direcciones IP de mi red o subred pudieran

estar al otro lado de la *internetwork* respecto a mi computadora, los routers de la red podrían enviar incorrectamente algunos de los paquetes enviados a mi computadora al otro lado de la red.

Clases de redes

La RFC 791 define el Protocolo IP, incluyendo varias clases diferentes de redes. IP define tres clases de redes diferentes para las direcciones que los hosts individuales utilizan: direcciones denominadas direcciones IP de unidifusión. Estas tres clases de redes son A, B y C. TCP/IP también define direcciones de clase D (multidifusión) y direcciones de clase E (experimentales).

Por definición, todas las direcciones de la misma red de clase A, B o C tienen el mismo valor numérico en la porción de red de las direcciones. El resto de la dirección es lo que se conoce como parte de host de la dirección.

Cada una de las redes de clase A, B y C tiene una longitud diferente para la parte que identifica la red:

- Cada una de las redes de clase A tiene una parte de red con una longitud de 1 byte. Esto deja 3 bytes para el resto de la dirección, la parte del host.
- Las redes de clase B tienen una parte de red de 2 bytes de longitud, dejando 2 bytes para la parte del host de la dirección.
- Las redes de clase C tienen una parte de red con una longitud de 3 bytes, dejando únicamente 1 byte para la parte de host.

Cuando se necesitan números de red, la convención es escribir la parte de red del número y rellenar con ceros decimales la parte de host del mismo. Ahora considere el tamaño de cada clase de red. Las redes de clase A necesitan 1 byte para la parte de red, dejando 3 bytes, o 24 bits para la parte de host. Existen 2^{24} valores posibles diferentes en la parte de host de una dirección IP clase A. por tanto, cada red de clase A puede tener 2^{24} direcciones IP (excepto las dos direcciones de host reservadas en cada clase. La siguiente tabla resume las características de las redes de clase A, B y C.

Cualquier red de esta clase	Número de bytes de red (bits)	Número de bytes de *host (bits)*	Número de direcciones por red*
A	1 (8)	3(24)	$2^{24} - 2$
B	2 (16)	2 (16)	$2^{16} - 2$
C	3 (24)	1 (8)	$2^{8} - 2$

Tabla 8.2 Tamaños de las partes de red y de *host* de las direcciones IP sin *subnetting*.

* Hay dos direcciones de *host* reservadas por cada red.

Aunque los números de red se parecen a las direcciones debido a su formato decimal con puntos, los números de red no pueden ser asignados a una interfaz para ser utilizados como una dirección IP. Conceptualmente, los números de red representan el grupo de todas las direcciones IP de la red. Sería confuso que un sólo número representara un grupo completo de direcciones y que también utilizase ese mismo número como una dirección IP para un dispositivo individual. Por tanto. Los propios números de red están reservados y no pueden utilizarse como dirección IP para un dispositivo.

Además del número de red, en cada red está reservado un segundo valor decimal con puntos. El primer valor reservado, el número de red, está relleno con ceros binarios en la parte del host del número. El otro valor se denomina dirección de difusión de red o de difusión dirigida. Este número reservado no puede ser asignado a un host para su uso como una dirección IP. No obstante, los paquetes remitidos a una dirección de difusión de red son enviados a todos los dispositivos de la red.

Como el número de red es el valor numérico más pequeño dentro de la red y la dirección de difusión es el valor numérico más alto, todos los números entre el número de red y la dirección de difusión son las direcciones IP válidas y útiles que se pueden utilizar para dirigir las interfaces de la red.

Los números de red de clase A, B y C

Internet es una colección de casi todas las redes basadas en IP y casi todas las computadoras host TCP/IP del mundo. El diseño original de Internet requería varias características de cooperación que lo hicieron posible técnicamente así como administrativamente manejable:

- Toda computadora conectada a Internet necesita una dirección IP única y no duplicada.
- Administrativamente, una autoridad central asignó redes de clase A, B y C a empresas, gobiernos, sistemas universitarios y Proveedores de Servicios de Internet (ISPs, *Internet Service Providers*) basándose en el tamaño de su red IP (clase A para las redes más grandes, clase B para las redes medianas y clase C para las redes más pequeñas).
- La autoridad central asignó cada número de red únicamente a una organización, lo que ayudó a garantizar la asignación de direcciones únicas a nivel mundial.
- Cada organización con una red de clase A, B o C asignada, asigna después direcciones IP individuales dentro de su propia red.

Siguiendo estas directrices, mientras cada organización asigne cada dirección IP sólo a una computadora, toda computadora en Internet tendrá una dirección IP globalmente única.

La organización a cargo de la asignación universal de direcciones IP es ICANN (*Internet Corporation for Assigned Network Numbers*). ICANN a su vez, asigna la autoridad regional a otras organizaciones cooperantes. Por ejemplo, el *American Registry for Internet Numbers* (ARIN) posee el proceso de asignación de direcciones para Norteamérica.

La siguiente tabla resume los posibles números de red que la ICANN y otras agencias podrían asignar con el tiempo.

Clase	Rango del primer octeto	Número de red válidos	Número total para esta clase de red	Número de hosts por red
A	1 a 126	1.0.0.0 a 126.0.0.0	2^7 - 2 (126)	2^{24} – 2 (16.777.214)
B	128 a 191	128.0.0.0 a 191.255.0.0	2^{14} (16.384)	2^{16} – 2 (65.534)
C	192 a 223	192.0.0.0 a 223.255.255.0	2^{21} (2.097.152)	2^8 – 2 (254)

Tabla 8.3 Todos los números de red válidos posibles.

La columna Números de red válidos muestra los números de red reales. Las redes 0.0.0.0 (todavía disponible para su uso como una dirección de difusión) y 127.0.0.0 (todavía disponible para su uso como la dirección de *loopback*) están reservadas.

La columna Números de red válidos muestra los números de red reales. Las redes 0.0.0.0 (originalmente definida para su uso como una dirección de difusión) y 127.0.0.0 (todavía disponible para su uso como la dirección de *loopback*) están reservadas.

9. Subnetting IP

El *subnetting* es una de los temas que motivaron el desarrollo de este proyecto, además de ser una práctica de gran demanda en la industria de las Tecnologías de la Información y Comunicaciones (TICs),

Por definición, una dirección IP que empieza por 8 en el primer octeto está en una red de clase A, por lo que la parte de red de la dirección es el primer byte, o primer octeto. Una dirección que empieza con 130 está en una red de clase B. Por definición, las direcciones de clase B tienen una parte de red de 2 bytes. Por último, una dirección que empieza con 199 está en una red de clase C, que tiene una parte de red de 3 bytes. También por definición, una dirección de clase A tiene una parte de host de 3 bytes, una de clase B tiene una parte de host de 2 bytes y una de clase C tiene una parte de host de 1 byte.

Las computadoras utilizan una máscara para definir el tamaño de las partes de red y de host de una dirección. La lógica que hay detrás de la máscara da como resultado las mismas convenciones de las redes de clase A, B y C que ya conocemos, pero la computadora puede tratarlo mejor como un problema matemático binario.

La máscara es un número binario de 32 bits, que normalmente se escribe en formato decimal con puntos. El objetivo de la máscara es definir la estructura de una dirección IP. Por lo tanto, la máscara define el tamaño de la parte de host de una dirección IP, quedando representada esta parte con ceros (0) binarios en la máscara. La primera parte de la máscara contienen unos (1) binarios, que representan la parte de red de las direcciones (si no se utiliza el *subnetting*), o las partes de red y de host de las direcciones (si se utiliza el *subnetting*).

Cuando no se utiliza el *subnetting*, cada clase de dirección IP utiliza la máscara predeterminada para esa clase. La siguiente tabla resume las máscaras predeterminadas y refleja el tamaño de las dos partes de una dirección IP.

Clase de dirección	Tamaño de la parte de red de la dirección en bits	Tamaño de red de la parte de *host* de la dirección en bits	Máscara predeterminada para cada clase de red
A	8	24	255.0.0.0
B	16	16	255.255.0.0
C	24	8	255.255.255.0

Tabla 9.1 Redes de clase A, B y C: partes de red y de host y máscaras predeterminadas.

Direccionamiento público y privado

El ICANN y las organizaciones asociadas gestionan el proceso de asignación de los números de red IP, como anteriormente mencionamos, o incluso los rangos más pequeños de direcciones IP, a las empresas que quieren conectarse a Internet. Después de que una empresa se le asigna un rango de direcciones IP, sólo esa empresa puede utilizar ese rango. Además, los routers de Internet pueden aprender después rutas para llegar a estas redes, para que todos en toda la Internet puedan enviar paquetes a esa red IP. Como estas direcciones IP pueden ser alcanzadas por paquetes en la Internet, estas se denominan a menudo redes públicas, y las direcciones de esas redes se llaman direcciones públicas.

Algunas computadoras nunca se conectarán a Internet. Por tanto, los ingenieros que instalaran una red compuesta únicamente de dichas computadoras podrían utilizar direcciones IP duplicadas de las direcciones IP públicas registradas en Internet. Así pues, al diseñar la convención de direccionamiento IP para una red semejante, una empresa podría elegir y utilizar los números que quisiera, y sería correcto.

No obstante, el usar las mismas direcciones IP que otra empresa es innecesario en esta situación, porque la RFC 1918 TCP/IP define un conjunto de redes privadas que pueden utilizarse para las *internetworks* que no se conectan a Internet. Y lo que es más importante, este conjunto de redes privadas nunca serán asignadas por el ICANN a ninguna empresa para que las utilice como números de red pública registrados. Así, al construir una red privada, como la de un laboratorio, se puede

utilizar números de un rango que nadie utiliza en la Internet pública. La siguiente tabla muestra el espacio de direcciones privadas definido por la RFC 1918.

Redes IP privadas	Clase de redes	Número de redes
10.0.0.0 hasta 10.0.0.0	A	1
172.16.0.0 hasta 172.31.0.0	B	16
192.168.0.0 hasta 192.168.255.0	C	256

Tabla 9.2 Espacio de direcciones privadas definido por la RFC 1918.

Cualquier empresa puede utilizar estos números de red. Sin embargo, ninguna empresa tiene permiso para publicar estas redes utilizando un protocolo de enrutamiento en Internet.

El *subnetting* IP crea grandes cantidades de grupos más pequeños de direcciones IP, en comparación con usar únicamente las convenciones de clase A, B y C. Se puede seguir pensando en las reglas de las clases A, B y C, pero ahora una sola red de clase A, B o C puede subdividirse en muchos grupos más pequeños. El *subnetting* procesa la subdivisión de una red de clase A, B o C como si esa subdivisión fuera una red. Para ello, una red de clase A, B o C se puede subdividir en muchas subredes no superpuestas.

Con el *subnetting*, la tercera parte de una dirección IP (la parte de subred) aparece en medio de la dirección. Este campo se crea “robando” o “tomando prestados” bits de la parte de host de la dirección. El tamaño de la parte de red de la dirección nunca se reduce. En otras palabras, siguen aplicándose las reglas de las clases A, B y C al definir el tamaño de la parte de red de una dirección. No obstante, la parte de host de la dirección se reduce a fin de dejar espacio para la parte de subred de la dirección.

El enrutamiento IP y el direccionamiento IP se diseñaron teniendo en mente a ambos. El enrutamiento IP presume de la estructura del *subnetting* IP, en la que los rangos de direcciones IP consecutivas residen en una sola subred. La RFCs de

direccionamiento IP definen el *subnetting* para que esas direcciones IP consecutivamente numeradas se puedan representar como una número de subred (dirección y subred) y una máscara de subred. De este modo, los routers pueden enumerar suficientemente las subredes en sus tablas de enrutamiento. Los routers necesitan una buena forma de listar en número de subred en sus tablas de enrutamiento. Esta información debe implicar de algún modo las direcciones IP de la subred.

Notación con prefijo / notación CIDR

Las máscaras de subred son, en realidad, números de 32 bits, pero por comodidad, normalmente se escriben como números decimales con puntos; por ejemplo, 255.255.0.0. Sin embargo, otra forma de representar una máscara, la notación con prefijo (en ocasiones también denominada notación de Encaminamiento Inter-Dominios sin Clases (CIDR, *Classless Inter-Domain Routing*), ofrece una forma aún más breve de escribir o de expresar una máscara de subred. Para comprender la notación con prefijo es importante saber que todas las máscaras de subred tienen alguna cantidad de 1s binarios consecutivos, seguidos de 0s binarios. Es decir, una máscara de subred no puede tener 1s y 0s intercalados. La máscara siempre tiene alguna cantidad de 1s binarios, seguidos únicamente por 0s binarios.

Con el fin de escribir la máscara de subred, la notación con prefijo indica el número de 1s binarios de una máscara, precedido por una /. Por ejemplo, para la máscara de subred 255.255.255.0, cuyo equivalente binario es 11111111 11111111 11111111 00000000, la notación con prefijo equivalente es /24, porque en la máscara hay 24 1s binarios consecutivos.

Análisis y selección de máscaras de subred

El proceso se *subnetting* subdivide una red con clase (una red de clase A, B o C) en grupos de direcciones más pequeños, denominados subredes. Cuando un ingeniero diseña una *internetwork*, a menudo decide usar una sola máscara de subred en una red con clase particular. La elección de la máscara de subred resuelve algunos de

los requisitos clave del diseño; por ejemplo, la necesidad de cierto número de subredes, y alguna cantidad de hosts por subred. La elección de la máscara de subred define después la cantidad de subredes de esa red con clase que puede existir, y cuántas direcciones de host existen en cada subred, así como las subredes específicas.

Partes de una dirección IP

Las redes de clase A, B y C tienen 8, 16 ó 24 bits en sus campos de red, respectivamente. Estas reglas no cambian. Sin el *subnetting* las direcciones de clase A, B y C tienen 24, 16, u 8 bits en sus campos de *host*, respectivamente. Con la técnica del *subnetting*, la parte de red de la dirección no se reduce o cambia, pero el campo de *host* se reduce para hacer sitio al campo de subred. A continuación se muestran algunas indicaciones para deducir el tamaño de las partes de red, subred y *host* de una dirección IP:

- La parte de red de la dirección siempre está definida por las reglas de la clase.
- La parte de host de la dirección siempre está definida por la máscara de subred. El número de 0s binarios de la máscara (siempre dispuestos al final de la misma) define el número de bits de host de la parte de host de la dirección.
- La parte de subred de la dirección es el sobrante de la dirección de 32 bits.

En conclusión, el *subnetting* nos permite resolver los problemas de escalabilidad de dos maneras. Primero, mejora nuestra eficiencia en la asignación de direcciones permitiendo no utilizar una nueva dirección Clase C o Clase B cada vez que necesitemos agregar una nueva red física. Segundo, nos ayuda a agregar información. Desde una distancia razonable, una colección compleja de redes físicas puede hacerse ver como una red sencilla, logrando así que la cantidad de información que los routers necesitan para enviar datagramas a esas redes sea reducida.

10. LANs Virtuales

Conceptos

Las LANs se pueden concebir en diversas perspectivas. Una LAN incluye todos los dispositivos del mismo dominio de difusión. Un dominio de difusión incluye el conjunto de todos los dispositivos conectados a la LAN que cuando un dispositivo envía una trama de difusión, todo los demás dispositivos la reciben. Por tanto, se puede pensar que una LAN y un dominio de difusión son la misma cosa.

Sin VLANs, un switch considera que todas sus interfaces están en el mismo dominio de difusión; en otras palabras, todos los dispositivos conectados están en la misma LAN. Con VLANs, un switch puede poner algunas interfaces en el mismo dominio de difusión que otras, creando múltiples dominios de difusión. Estos dominios de difusión individuales creados por el switch se denominan LANs virtuales.

Situar *hosts* en dos VLANs diferentes proporcionan muchos beneficios, aunque las razones pueden no ser obvias. La clave para apreciar estos beneficios es comprender que una difusión enviada por un host en la VLAN será recibida y procesada por todos los demás *hosts* de la VLAN, pero no por los hosts de una VLAN diferente. Cuantos más hosts haya en una VLAN dada, mayor será el número de difusiones y por tanto mayor será el tiempo de procesamiento que va a requerir cada uno de los hosts de esa VLAN. Además cualquiera puede obtener paquetes de software libre, llamados genéricamente analizadores de protocolos, con los cuales capturar todas las tramas recibidas por un host. Como resultado, las grandes VLANs producen gran número y tipos de difusiones a los otros equipos, produciendo más tramas en los hosts que podrían ser usadas por un atacante que utilice un software analizador de protocolos para tratar de realizar un ataque.

Éstas son sólo algunas razones para separar los hosts en VLANs diferentes. Las razones más comunes son las siguientes:

- Crear diseños más flexibles que agrupen a usuarios por departamentos, o por grupos que trabajen juntos, en lugar de por su ubicación física.
- Segmentar dispositivos en LANs más pequeñas (dominios de difusión) para reducir la sobrecarga causada por cada host en la VLAN.
- Reducir la carga de trabajo del Protocolo de árbol de extensión (STP, *Spanning Tree Protocol*) limitando a una VLAN a un único acceso al switch.
- Forzar una mayor seguridad separando los hosts que trabajen con datos sensibles en una VLAN diferente.
- Separar tráfico enviado por un teléfono IP del tráfico enviado por PCs conectados a los teléfonos.

Trunking con ISL y 802.1Q

Cuando se utilizan VLANs en una red con varios switches interconectados, los switches debes usar el *trunking* VLAN en los segmentos entre los switches. Este proceso permite a los switches utilizar el proceso denominado etiquetado de VLAN (*VLAN tagging*), por el cual el switch emisor añade otro encabezado a la trama antes de enviarla por el troncal. Este encabezado VLAN extra incluye un campo identificador de VLAN (ID VLAN) por el cual el switch emisor puede mostrar el ID de la VLAN y el switch receptor puede entonces conocer a qué VLAN pertenece cada trama. El uso del *trunking* permite a los switches pasar varias tramas procedentes de varias VLANs a través de una única conexión física.

Los switches de Cisco soportan dos protocolos diferentes de *trunking*: enlace entre switches (ISL, *Inter-Switch Link*) e IEEE 802.1Q. Los protocolos de *trunking* proporcionan varias características, la más importante de ellas define las cabeceras con las cuales identificar el ID VLAN.

ISL

Cisco creó ISL varios años antes que el IEEE creara el protocolo de *trunking* estándar de VLAN, el 802.1Q. Debido a que ISL es propiedad de Cisco, sólo puede ser utilizado entre dos switches de Cisco que soporten ISL. ISL encapsula completamente la trama Ethernet original en una cabecera y una información final ISL. La trama Ethernet original dentro de la cabecera y la información final de ISL permanece inalterada. La siguiente figura muestra el entramado ISL.

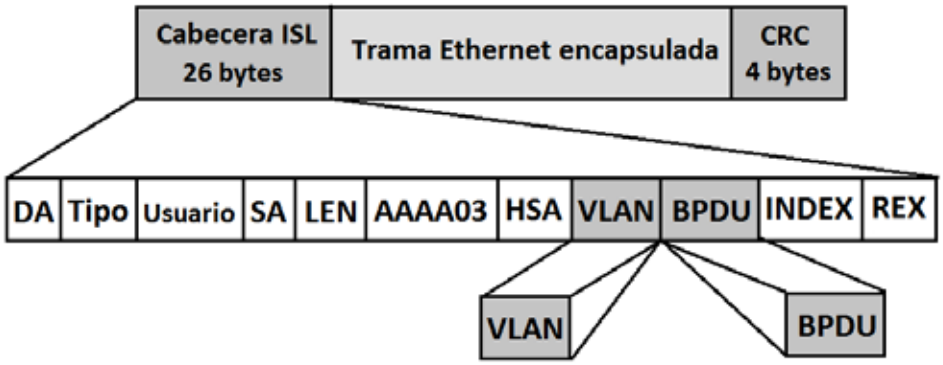


Figura 10.1 Cabecera Ethernet con entramado ISL.

La cabecera ISL incluye varios campos, pero lo más importante es que el campo VLAN de la cabecera ISL proporciona un lugar para codificar el número de VLAN. Etiquetando una trama con el número correcto de VLAN en la cabecera, el switch que envía puede asegurar que el switch receptor conoce a qué VLAN pertenece la trama encapsulada. También las direcciones de origen y destino en la cabecera ISL utilizan las direcciones MAC del switch que envía y del que recibe, en oposición a los dispositivos que realmente envían la trama original.

IEEE 802.1Q

El IEEE estandariza muchos de los protocolos relativos a las LAN. Hoy, 802.1Q ha llegado a ser el más popular de los protocolos de *trunking*. Cisco ya no soporta ISL en algunos de sus nuevos modelos de switches para LAN, incluyendo los switches 2960 utilizados en este proyecto.

802.1Q utiliza un estilo diferente de cabecera que el utilizado por ISL para etiquetar las tramas con un número de VLAN. De hecho, 802.1Q no encapsula realmente la trama original en otra cabecera y otra información final Ethernet. En cambio, 802.1Q inserta una cabecera de VLAN extra de 4 bytes en la cabecera Ethernet de la trama original. Como resultado, al contrario de ISL, la trama tiene todavía las direcciones MAC de origen y destino originales. También, debido a que la cabecera original se ha expandido, la encapsulación de 802.1Q fuerza a recalcular el campo de secuencia de verificación de trama (FCS) en la información final Ethernet, debido a que este campo está basado en el contendido de la trama completa. La siguiente figura muestra la cabecera 802.1Q y el entramado de la cabecera Ethernet revisada.

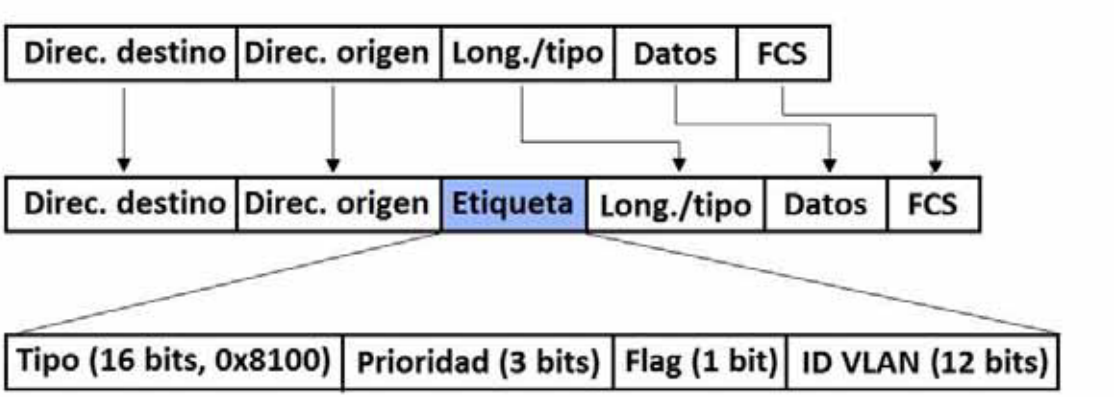


Figura 10.2 Cabecera 802.1Q y entramado de la cabecera Ethernet.

Comparación de ISL con 802.1Q

La similitud es que ambos definen una cabecera VLAN que tiene un campo ID VLAN. No obstante, cada uno de los protocolos de *trunking* utiliza una cabecera de sobrecarga diferente, y uno está estandarizado (802.1Q) y otro es propietario (ISL). Ambos protocolos soportan el mismo número de VLANs, concretamente 4094 VLANs. Ambos utilizan 12 bits de la cabecera de VLAN para numerar las VLANs, soportando 2^{12}, ó 4096, IDs de VLAN, menos dos valores reservados (0 y 4095). De las VLANs soportadas, los IDs de VLAN, de 1-1005 se consideran el "rango normal" de VLANs, mientras que los valores mayores de 1005 se denominan "rango extendido" de VLANs. Esta discusión está relacionada con el Protocolo *trunking* VLAN (VTP, *VLAN Trunking Protocol*).

ISL y 802.1Q soportan ambos una instancia separada del Protocolo de Árbol de Extensión (STP, *Spanning Tree Protocol*) para cada VLAN, pero con diferentes detalles de implementación. Para las LANs de campus con enlaces redundantes, el uso de una única instancia de STP significa que algunos de los enlaces permanecen inactivos en su modo normal de operación. Estos enlaces sólo se utilizan cuando otro falla. Soportando múltiples instancias de STP, los ingenieros pueden ajustar los parámetros de STP para que bajo un funcionamiento normal, parte del tráfico de las VLANs utilice un conjunto de enlaces y otro tráfico de las VLANs utilice otros enlaces, con la ventaja de usar así todos los enlaces de la red.

Una diferencia clave entre ISL y 802.1Q está relacionada con una característica denominada **VLAN nativa**. 802.1Q define una VLAN en cada troncal como la VLAN nativa, mientras que ISL no utiliza este concepto. Por defecto, la VLAN nativa de 802.1Q es la VLAN 1. Por definición, 802.1Q simplemente no añade una cabecera 802.1Q a las tramas de la VLAN nativa. Cuando un switch del otro lado del troncal recibe una trama que no tiene una cabecera 802.1Q, el switch receptor sabe que la trama pertenece a la VLAN nativa. Debido a esta conducta, ambos switches deben estar de acuerdo en qué VLAN es la nativa.

La VLAN nativa de 802.1Q proporciona algunas funciones interesantes, principalmente la conexión de dispositivos que no soportan el *trunking*. Por ejemplo, un switch Cisco podría estar conectado a un switch que no soporte el *trunking*

802.1Q. El switch de Cisco podría enviar tramas en la VLAN nativa (significa que la trama no tiene cabecera de *trunking*); por tanto, el otro switch podría entender la trama. El concepto de VLAN nativa proporciona a los switches la capacidad de reenviar tráfico de una VLAN (la VLAN nativa), lo que puede permitir algunas funciones básicas como la accesibilidad vía telnet de un switch.

En la siguiente tabla se resumen las características claves y los puntos de comparación entre ISL y 802.1Q.

Función	**ISL**	**802.1Q**
Definida por	Cisco	IEEE
Inserta otros 4 bytes en la cabecera en vez de encapsular completamente la trama original	No	Sí
Soporta rango normal (1-1005) y extendido (1006-4094) de VLANs	Sí	Sí
Permite múltiples árboles de extensión	Sí	Sí
Utiliza VLAN nativa	No	Sí

Tabla 10.1 Comparación ISL y 802.1Q.

Subredes IP y VLANs

Al incluir VLANs en un diseño, los dispositivos de una VLAN necesitan estar en la misma subred. Siguiendo la misma lógica de diseño, los dispositivos en VLANs diferentes necesitan pertenecer a subredes diferentes.

Debido a estas reglas, mucha gente piensa que una VLAN es una subred y una subred una VLAN. Lo cual no es completamente cierto, porque una VLAN es un concepto de la capa 2 y una subred es un concepto de la capa 3, la idea general es razonable porque los mismos dispositivos en una única VLAN son los mismos dispositivos en una única subred.

Como en todas las subredes IP, para que un *host* en una subred puede entregar paquetes a otro host en otra subred, al menos un router debe estar involucrado.

Vlan Trunking Protocol (VTP)

El VTP propietario de Cisco proporciona un mecanismo por el cual los switches de Cisco pueden intercambiar información de la VLAN. En concreto, VTP publica sobre la existencia de cada VLAN basándose en el ID y el nombre de la VLAN. No obstante, VTP no publica los detalles sobre que interfaces del switch están asignadas a cada VLAN.

VTP define un protocolo de mensajes de capa 2 que los switches utilizan para intercambiar información sobre la configuración de la VLAN. Cuando un switch cambia su configuración de VLAN (en otras palabras, cuando se añade o borra una VLAN, o cambia una ya existente) VTP sincroniza la configuración VLAN de todos los switches incluyendo los mismo IDs y nombres de VLAN. El proceso es similar a un protocolo de enrutamiento con cada switch enviando periódicamente mensajes VTP. Los switches también envían mensajes tan pronto como su configuración de VLAN cambia. Por ejemplo, si se configura una nueva VLAN con el nombre de PUBLICIDAD, el switch enviará inmediatamente una actualización de VTP por todos los troncales, permitiendo la distribución de la información de la nueva VLAN al resto de los switches.

Cada switch utiliza uno de los tres modos de VTP: modo servidor, modo cliente, o modo transparente. Entonces se añade la configuración de la VLAN PUBLICIDAD en este servidor y lo demás switches configurados previamente como clientes aprenden acerca de los cambios en la base de datos de VLAN. Los clientes no se pueden utilizar para configurar la información VLAN.

Los switches Cisco no pueden deshabilitar VTP. La opción más parecida es utilizar el modo transparente, lo que causa que el switch ignore VTP, con la excepción de reenviar los menajes VTP hacia otros clientes y servidores.

Pruning VTP

Por default, los switches Cisco inundan las difusiones y las direcciones de destino desconocidas de cada VLAN activa por todos los troncales, mientras la topología actual de STP no bloquee el troncal (STP se verá más adelante). Sin embargo, en la mayoría de las redes de campus, existen muchas VLAN en sólo unos pocos switches, no en todos. Por tanto, está de más enviar las difusiones por todos los troncales, provocando que las tramas lleguen a los switches que no tienen ningún puerto en esa VLAN.

Los switches soportan dos métodos con los que un ingeniero puede limitar el flujo de tráfico de la VLAN en un troncal. Uno de ellos necesita la configuración manual de la lista VLAN permitida en cada troncal. El segundo método, el *pruning* VTP, permite a VTP determinar dinámicamente qué switches no necesitan tramas de ciertas VLANs, y entonces VTP recorta estas VLANs en los troncales adecuados. El concepto de *pruning* simplemente significa que las interfaces apropiadas del troncal del switch no inundan tramas de esa VLAN.

El *pruning* VTP incrementa el ancho de banda disponible restringiendo el tráfico inundando. El *pruningK* VTP es una de las dos razones principales para el uso de VTP, siendo la otra el hacer la configuración de la VLAN más fácil y consistente.

VLANs y troncales seguros

Los switches están expuestos a varios tipos de vulnerabilidades de seguridad tanto en los puertos utilizados como en los que no. Por ejemplo, un atacante podría conectar una computadora a un punto de cableado de red que está conectado a un puerto de un switch y causar problemas en la VLAN asignada a ese puerto. Además, el atacante podría negociar el *trunking* y causar muchos otros tipos de problemas, algunos relacionados con VTP.

Esto se puede lograr con diferentes mecanismos de configuración que protegen a los puertos no utilizados de un switch. En lugar de utilizar los valores predeterminados, Cisco recomienda configurar estas interfaces como sigue:

- Deshabilitar administrativamente la interfaz no utilizada.
- Prevenir la negociación del *trunking*.
- Asignar el puerto a una VLAN no utilizada.

Con cerrar las interfaces sería más que suficiente, sin embargo, las otras dos tareas previenen cualquier problema inmediato si por algún motivo se habilita la interfaz.

Después de estas recomendaciones para los puertos no utilizados, Cisco recomienda deshabilitar la negociación del *trunking* en todas las interfaces en uso, configurando todos los troncales manualmente. La exposición es que un atacante podría desconectar la computadora de un usuario legítimo del puerto RJ-45, conectando su computadora y tratar de negociar el troncal. Configurando todas las interfaces utilizadas para no negociar el troncal, estas interfaces no podrían decidir dinámicamente un troncal, reduciendo la exposición a problemas relacionados con el *trunking*. Para cualquier interfaz local, Cisco recomienda su configuración manual.

11. Protocolo de Árbol de Extensión (IEEE 802.1D)

En algunos diseños de LANs se necesitan múltiples switches, la mayoría de los ingenieros de redes incluyen segmentos Ethernet redundantes entre ellos. El objetivo es sencillo. Lo switches podrían fallar, y los cables podrían cortarse o desenchufarse; si se instalan switches y cables redundantes, el servicio de red podría permanecer disponible para la mayoría de los usuarios.

Las LANs con enlaces redundantes introducen la posibilidad de que las tramas puedan formar pos siempre bucles en la red. Estas tramas podrían causar problemas en el rendimiento de la red. Por tanto, las LANs utilizan el Protocolo de Árbol de Extensión (STP, *Spanning Tree Protocol*), el cual permite el uso de enlaces LAN redundantes mientras previene que las tramas formen bucles indefinidamente alrededor de la LAN a través de estos enlaces redundantes.

Con STP habilitado, algunos switches bloquean puertos para que esos puertos no reenvíen las tramas. STP selecciona qué puertos bloqueará de forma que sólo exista un camino activo entre cualquier par de segmentos de LAN (dominios de colisión). Como resultado las tramas alcanzan cada dispositivo sin causar los problemas creados cuando las tramas forman bucles en la red.

Necesidad del árbol de extensión

El problema más común que puede ser evitado con el uso de STP es el de las tormentas de difusión. Las tormentas de difusión causan que las difusiones (o multidifusiones o unidifusiones con dirección de destino desconocida) formen bucles indefinidamente en una LAN. Como resultado, algunos enlaces pueden llegar a saturarse con copias inútiles de la misma trama, dejando fuera tramas buenas, así como provocar un impacto significativo en el rendimiento de las PCs de usuario final al provocar que procesen demasiadas tramas de difusión.

Los switches inundan las difusiones por todas las interfaces de la misma VLAN, excepto por la que llegó la trama. Como resultado de estos bucles también se produce inestabilidad en las tablas MAC. La inestabilidad en la tabla MAC significa

que las tablas de direcciones MAC de los switches seguirán cambiando la información especificada para la dirección MAC de origen de las tramas en bucle.

La tercera clase de problemas causados por no utilizar STP en una red con redundancia es que los hosts que funcionan toman múltiples copias de la misma trama, los switches inundan las tramas dirigidas a una dirección MAC desconocida.

La siguiente tabla resume las tres clases de problemas principales que ocurren cuando no se utiliza STP en una LAN con redundancia.

Problema	**Descripción**
Tormentas de difusión	El reenvío repetido de una trama en los mismos enlaces consume una parte significativa de las capacidades de los enlaces.
Inestabilidad en la tabla MAC	La actualización continua de la tabla de direcciones MAC de un switch con entradas incorrectas, como reacción a las tramas que entran en bucle, provoca que las tramas sean enviadas a localizaciones incorrectas.
Transmisión múltiple de la trama	Un efecto colateral de las tramas que entran en bucle en el cual múltiples copias de la misma trama se entregan al host previsto, confundiéndolo.

Tabla 11.1 Clases de problemas en un LAN con redundancia sin STP.

Función del Árbol de Extensión

STP previene bucles colocando cada puerto de un switch en estado de Envío o en estado de Bloqueo. Las interfaces en estado de Envío actúan normalmente, reenviando y recibiendo tramas, pero las interfaces en estado de Bloqueo no procesan tramas excepto los mensajes STP. Se considera que todos los puertos en estado de Envío están en el árbol de extensión actual. El conjunto colectivo de puertos de reenvío crea un camino único por el cual se envían las tramas entre segmentos Ethernet.

Operación del Árbol de Extensión

El algoritmo STP crea un árbol de extensión de interfaces que reenvían tramas. La estructura de árbol crea un camino único a y desde cada segmento Ethernet, simplemente como se puede trazar un camino único hacia una hoja, creciendo el árbol desde su base a cada hoja.

El proceso utilizado por STP, a veces denominado **Algoritmo de árbol de extensión** (STA, *Spanning Tree Algorithm*), selecciona las interfaces que serán colocadas en un estado de Envío. Para cualquier interfaz no seleccionada para estar en este estado, STA coloca las interfaces en estado de Bloqueo. Con otras palabras, STP simplemente elige qué interfaces reenviarán.

STP utiliza tres criterios para seleccionar si colocar una interfaz en estado de Envío o de Bloqueo:

- STP elige un switch raíz. STP coloca esta interfaz de mínimo coste al raíz, llamada **puerto raíz** (RP, *Root Port*) del switch, en estado de Envío.
- Muchos switches pueden estar conectados al mismo segmento Ethernet. El switch con el costo administrativo más bajo desde sí mismo hasta el puente raíz, comparando con los otros switches conectados al mismo segmento, se coloca en estado de Envío. El switch de menor costo en cada segmento es llamado **puente designado**, y la interfaz del puente conectada a ese segmento se denomina **puerto designado** (DP, *Designated Port*). Todas las demás interfaces se configuran en estado de Bloqueo.

La siguiente tabla resume las razones de STP para configurar en estado de Envío o de Bloqueo.

Caracterización del puerto	Estado STP	Descripción
Todos los puertos del switch raíz	Envío	El switch raíz es siempre el switch designado en todos los segmentos a los que está conectado.
Cada puerto raíz de un switch que no es raíz	Envío	El puerto a través del cual el switch tiene el menor coste para alcanzar el switch raíz.
Cada puerto designado de la LAN	Envío	El switch que reenvía la BPDU de menor coste por el segmento es el switch designado para ese segmento.
Todos los demás puertos operativos	Bloqueo	El puerto no se utiliza para enviar tramas, ni se considerará ninguna trama recibida por estas interfaces para su envío.

Tabla 11.2 Razones de STP para configurar Envío o Bloqueo.

La ID de puente STP y la BPDU Hello

El Algoritmos de Árbol de Extensión (STA) comienza con la elección de un switch para ser el switch raíz. Para comprender mejor este proceso de elección, se necesita entender los menajes STP que se intercambian los switches, así como el concepto y formato del identificador utilizado para identificar de forma única cada switch.

El ID de puente (BID, *bridge ID*) de STP es un valor único de 8 bytes para cada switch. El ID de puente consta de un campo de prioridad de 2 bytes y un ID de sistema de 6 bytes, con el ID de sistema basado en una dirección MAC grabada en cada switch. El uso de una dirección MAC grabada asegura que cada Id de puente del switch sea único.

STP define mensajes llamados **Unidades de datos del protocolo de puente** (BPDU, *Bridge Protocol Data Units*), que utilizan los puentes y switches para intercambiar información entre ellos. El mensaje más común, llamado BPDU Hello, contiene el ID de puente del switch emisor. Indicando su propio y único ID de puente, los switches pueden diferenciar BPDUs enviadas desde diferentes switches. Este mensaje también contiene el ID puente del switch raíz actual.

STP define tipos de mensajes BPDU, con la BPDU Hello como mensaje que realiza la mayoría del trabajo. LA BPDU Hello incluye varios campos, los más importantes se listan a continuación.

Campo	**Descripción**
ID del puente raíz	El ID de puente del switch que el remitente de este mensaje Hello cree que es el switch raíz.
ID del puente emisor	El ID de puente del switch remitente de esta BPDU Hello.
Coste para alcanzar la raíz	El coste STP entre este swtich y la raíz actual.
Valor de los temporizadores en el switch raíz	Incluye el temporizador Hello, el temporizador de Edad máxima (*Max Age*) y el temporizador de Retardo de Envío (*Forward Delay*).

Tabla 11.3 Campos de BPDU Hello más importantes.

Switch raíz

Los switches eligen un switch raíz basándose en el ID de puente de las BPDUs. El switch raíz es el switch con el ID de puente de menor valor numérico. Ya que el ID de puente de dos partes comienza con el valor de prioridad, esencialmente el switch con la menor prioridad llega a ser la raíz. Por ejemplo, si uno de los switches tiene prioridad 100, y otro switch tiene prioridad 200, el switch con prioridad 100 gana, independientemente de qué dirección MAC se utilizará para crear el ID de puente para cada switch.

Si basándose en la porción de prioridad del ID de puente se produce un empate, el switch con la menor dirección MAC en la parte del ID de puente es la raíz. No será necesaria ninguna otra forma de romper el empate porque los switches utilizan sus propias direcciones MAC grabadas como la segunda parte de su ID de puente. Así, si hay empate de prioridades, y un switch utiliza la dirección MAC 0020.0000.0000 como parte del ID de puente, y el otro utiliza 0FFF.FFFF.FFFF, el primero llega a ser la raíz.

STP elige un switch raíz de una manera no muy distinta a una elección política. El proceso comienza con todos los switches demandando ser la raíz mediante el envío de BPDUs Hello conteniendo su propio ID de puente como el ID de puente raíz. Si un switch escucha un mensaje Hello que contiene un mejor (más bajo) ID de puente (llamado Hello superior) ese switch finaliza las publicaciones de sí mismo como raíz y comienza a enviar el Hello superior. El Hello enviado por el mejor switch contiene el ID de puente del mejor switch como la raíz. Trabaja como una carrera política en la cual el candidato menos popular se rinde y deja la carrera, dando su apoyo a otro candidato. Finalmente, cualquiera está de acuerdo con el switch que tiene el mejor (más bajo) ID de puente, y todos apoyan al switch elegido (que es donde la analogía de la carrera política se cae en pedazos).

Puerto raíz de cada switch

La segunda parte del proceso de STP tiene lugar cuando cada switch no raíz elige uno y sólo un puerto raíz. El puerto raíz de un switch (RP) es la interfaz a través de la cual tiene el menor costo de STP para alcanzar el switch raíz.

Para calcular el costo, un switch añade el costo contenido en un Hello recibido al costo del puerto STP asignado a la misma interfaz. El costo del puerto STP es simplemente un valor asignado a cada interfaz con el propósito de proporcionar una medida objetiva que permita a STP seleccionar qué interfaces añadir a la topología de STP.

Puerto designado en cada segmento LAN

El paso final de STP para elegir su topología es seleccionar el puerto designado en cada segmento de LAN. El puerto designado en cada segmento de LAN es el puerto del switch que publica el Hello de menor costo en un segmento de una LAN. Cuando un switch no raíz reenvía un Hello, el switch no raíz establece el campo de costo en el Hello al costo para alcanzar la raíz. En efecto, el switch con el menor costo para alcanzar la raíz, de entre todos los switches conectados a un segmento, llega a ser el DP en ese segmento. Todos los DPs se colocan en estado de envío. Si existe empate en las publicaciones de costo, los switches rompen el empate seleccionando el switch con el menor ID de puente.

Los costos de puerto pueden ser configurados, o utilizar los valores predeterminados. La tabla 11.4 muestra los costos de puerto predeterminados definidos por el IEEE; Cisco utiliza estos mismos valores. El IEEE revisó los valores de costo porque los valores originales, establecidos en los primeros años de los 80, no anticipaban el crecimiento de Ethernet para soportar 10 Gigabits.

Cuando se habilita STP, todas las interfaces operativas del switch establecerán un estado de Envío o de Bloqueo de STP, incluso los puertos de acceso. Para interfaces se switch conectadas a elementos o routers, que no utilizan STP, el switch enviará todavía Hellos por estas interfaces. Por la virtud de ser el único dispositivo enviando Hellos en ese segmento de LAN, el switch está enviando el Hello de costo mínimo en ese segmento de LAN, haciendo que el switch llegue a ser el puerto designado de ese segmento de LAN. Así, STP coloca a las interfaces de acceso que funcionan en un estado de Envío como resultado de la parte de puerto designado del proceso STP.

Velocidad Ethernet	Costo IEEE original	Costo IEEE revisado
10 Mbps	100	100
100 Mbps	10	19
1 Gbps	1	4
10 Gbps	1	2

Tabla 11.4 Costos de puerto predeterminados por el IEEE

Cómo reaccionar frente a cambios en la red

Una vez determinada la topología de STP (el conjunto de interfaces en estado de reenvío, este conjunto de interfaces no cambia a menos que cambie la topología de la red. Esta sección examina el funcionamiento continuado de STP mientras la red está estable, y después examina cómo STP converge a una nueva topología cuando algo cambia.

El switch raíz envía una nueva BPDU Hello cada 2 segundos (valor predeterminado). Cada switch reenvía el Hello por todos los DPs, pero sólo después de cambiar dos elementos. Se cambia el valor del costo para reflejar el costo del switch para alcanzar la raíz, y el campo de ID de puente del remitente. (El campo de ID de puente de la raíz no cambia.) Al enviar los Hellos recibidos (y cambiados) por todos lo DPs, todos los switches continúan recibiendo Hellos cada 2 segundos.

Cada switch confía en estos mensajes Hello periódicos recibidos desde la raíz como una manera de conocer que su camino a la raíz está todavía funcionando. Cuando un switch cesa de recibir los Hellos, algo ha fallado; por tanto, el switch reacciona y comienza el proceso de cambio de topología del árbol de extensión. Por varias razones, el proceso de convergencia requiere el uso de tres temporizadores. Todos los switches utilizan los temporizadores como dicta el switch raíz, temporizadores que la raíz incluye en sus menajes BPDU Hello periódicos.

Los temporizadores y sus descripciones se muestran en la siguiente tabla:

Temporizador	Descripción	Valor Predeterminado
Hello	Periodo de tiempo entre Hellos creados por la raíz.	2 segundos
Edad máxima	Cuánto debería esperar cualquier switch, después de no escuchar ya Hellos, antes de tratar de cambiar la topología de STP.	Hello 10 veces
Retardo de Envío	Retardo que afecta al proceso que ocurre cuando una interfaz cambia de estado de Bloqueo a estado de Envío. Un puerto permanece en un estado de escucha provisional, durante el número de segundos definido por el temporizador de retardo de reenvío.	15 segundos

Tabla 11.4 Costos de puerto predeterminados por el IEEE

Si el switch no recibe una esperada BPDU Hello en el tiempo Hello, el switch continúa normalmente. Sin embargo, si los Hellos no se presentan en el tiempo de Edad máxima, el switch reacciona realizando los pasos para cambiar la topología de STP. En este punto, el switch reevalúa qué switch podría ser el switch raíz, y si no es la raíz, qué puerto podría ser su RP, y qué puertos podrían ser DPs, asumiendo que los Hellos que fueron anteriormente recibidos han dejado de llegar.

Cuando un STP converge, un switch selecciona las interfaces que deben pasar de un estado a otro. Sin embargo, una transición de bloqueo a reenvío no puede ser realizada inmediatamente porque un cambio inmediato a reenvío podría causar que las tramas formaran bucles temporalmente. Para prevenir estos bucles temporales, en las transiciones STP, la interfaz pasa por dos estados intermedios, que son:

- **Escucha** (***Listening***): Igual que en el estado de Bloqueo, la interfaz no reenvía tramas. Las entradas antiguas e incorrectas de la tabla MAC han caducado durante este estado, debido a que dichas entradas podrían provocar bucles temporales.

- **Aprendizaje** (***Learning***): Las interfaces en este estado todavía no envían tramas, pero el switch comienza a aprender direcciones MAC de tramas recibidas por la interfaz.

STP cambia una interfaz de Bloqueo a Escucha, después a Aprendizaje, y después al estado de Envío. STP deja la interfaz en cada uno de estos estados interinos por un tiempo igual al del temporizador de retardo de reenvío. Como resultado, un evento de convergencia que causa el cambio de una interfaz de Bloqueo a Envío necesita 30 segundos para la transición de bloqueo a envío. Además, un switch podría tener que esperar los segundos de **edad máxima** antes incluso de decidir mover una interfaz del estado de Bloqueo al de Envío.

La siguiente tabla resume varios de los estados de las interfaces del Árbol de extensión para una fácil revisión.

Estado	¿Reenvía tramas de datos?	¿Aprende MACs basándose en las tramas recibidas?	¿Estado transitorio o estable?
Bloqueo	No	No	Estable
Escucha	No	No	Transitorio
Aprendizaje	No	Sí	Transitorio
Envío	Sí	Sí	Estable
Deshabilitado	No	No	Estable

Tabla 11.4 Costos de puerto predeterminados por el IEEE

12. EtherChannel, PortFast y BPDU Guard

STP tiene ya varios años operando en la industria de las redes, sin embargo, durante estos años, ha añadido características propietarias para introducir mejoras en STP. En algunos casos, el IEEE ha añadido estas mejoras, o algunas parecidas, a sus estándares posteriores, como una revisión del estándar como un estándar adicional. A continuación se examinaran tres añadidos propietarios a STP: EtherChannel, PortFast, y BPDU Guard.

EtherChannel

Una de las mejores maneras de disminuir el tiempo de convergencia de STP es evitar la convergencia completamente. EtherChannel proporciona una forma de prevenir la necesidad de la convergencia de STP cuando sólo ocurre un fallo en un único puerto o cable.

EtherChannel combina segmentos paralelos múltiples de igual velocidad (hasta ocho) entre el mismo par de switches, unidos en un EtherChannel. Los switches tratan al EtherChannel como una única interfaz a considerar en el proceso de reenvío de tramas y para STP. Como resultado, si uno de los enlaces falla, pero al menos uno de ellos está operando, la convergencia de STP no tiene que ocurrir.

Con cada par de enlaces Ethernet configurados como un EtherChannel, STP trata cada EtherChannel como un único enlace. En otras palabras, deben fallar ambos enlaces con el mismo switch para que el switch tenga que provocar la convergencia de STP. Sin EtherChannel, si se tienen enlaces paralelos múltiples entre dos switches, STP bloquea todos los enlaces excepto uno. Con EtherChannel, todos los enlaces paralelos pueden estar activos y funcionando al mismo tiempo, lo que aumenta la posibilidad de la red, mientras se reduce el número de veces que STP debe converger.

EtherChannel proporciona también mayor ancho de banda de red. Todos los troncales en un EtherChannel están o reenviando o bloqueados, debido a que STP trata a todos los troncales en el mismo EtherChannel como un único troncal.

Cuando un EtherChannel está en estado de Envío, los switches equilibran la carga de tráfico entre todos los troncales, proporcionando mayor ancho de banda.

PortFast

PortFast permite al switch colocar inmediatamente un puerto en estado de Envío cuando el puerto se activa físicamente, ignorando cualquier opción sobre la topología de STP e ignorando los estados de Escucha y Aprendizaje. Sin embargo, los únicos puertos en los que se puede habilitar PortFast de forma segura son aquellos que no conectan con puentes, switches, o cualquier otro dispositivo que hable STP.

PortFast es más apropiado para conexiones de dispositivos de usuario final. Si se establece PortFast en puertos conectados a dispositivos de usuario final, cuando el PC de un usuario final arranca, tan pronto como la NIC del PC se activa, el puerto del switch puede pasar al estado de Envío de STP y reenviar tráfico. Sin PortFast, cada puerto debe esperar mientras el switch confirma que el puerto es un DP, y entonces espera mientras la interfaz pasa por los estados temporales de Escucha y Aprendizaje.

Seguridad en STP

Las interfaces de un switch que conectan localizaciones de usuario final en la LAN tienen algunas exposiciones de seguridad. Un atacante podría conectar un switch a uno de estos puertos, con un valor de prioridad de STP bajo, y llegar a ser el switch raíz. También, conectando un switch pirata a múltiples switches legítimos, el switch pirata podría termina reenviando mucho tráfico en la LAN, y el atacante podría utilizar un analizador de LAN para copiar un gran número de tramas de datos enviadas a través de esa LAN. También, los usuarios podrían dañar involuntariamente la LAN. Por ejemplo, un usuario podría comprar y conectar un switch LAN barato de consumidor a otro switch existente, posiblemente creando un

bucle, o posiblemente provocando que el nuevo switch de potencia relativamente baja llegue a ser la raíz.

La característica de BPDU Guard de Cisco ayuda a evitar esta clase de problemas deshabilitando un puerto si se recibe por él una BPDU. Así, esta característica es particularmente útil en puertos que sólo se utilizarán como puerto de acceso y nunca conectados a otro switch. Además, la característica de BPDU Guard se utiliza a menudo en la misma interfaz que tiene habilitado PortFast, ya que un puerto con PortFast habilitado estará ya en un estado de Envío, lo que incrementa la posibilidad de bucles de envío.

La característica de Cisco Root Guard ayuda a evitar el problema cuando el nuevo switch (intruso) trata de llegar a ser el switch raíz. La prestación Root Guard permite que se pueda conectar a la interfaz otro switch, y participar en STP enviando y recibiendo BPDUs. Sin embargo, cuando la interfaz del switch con Root Guard habilitado recibe una BPDU superior del switch vecino (una BPDU con un ID de puente menor/mejor) el switch con Root Guard reacciona. No sólo ignora la BPDU superior, sino que el switch también deshabilita la interfaz, no enviando ni recibiendo tramas, mientras las BPDUs superiores sigan llegando. Si las BPDUs superiores dejan de llegar, el switch puede comenzar de nuevo a utilizar la interfaz.

13. Configuración del Proyecto Terminal

Preliminares

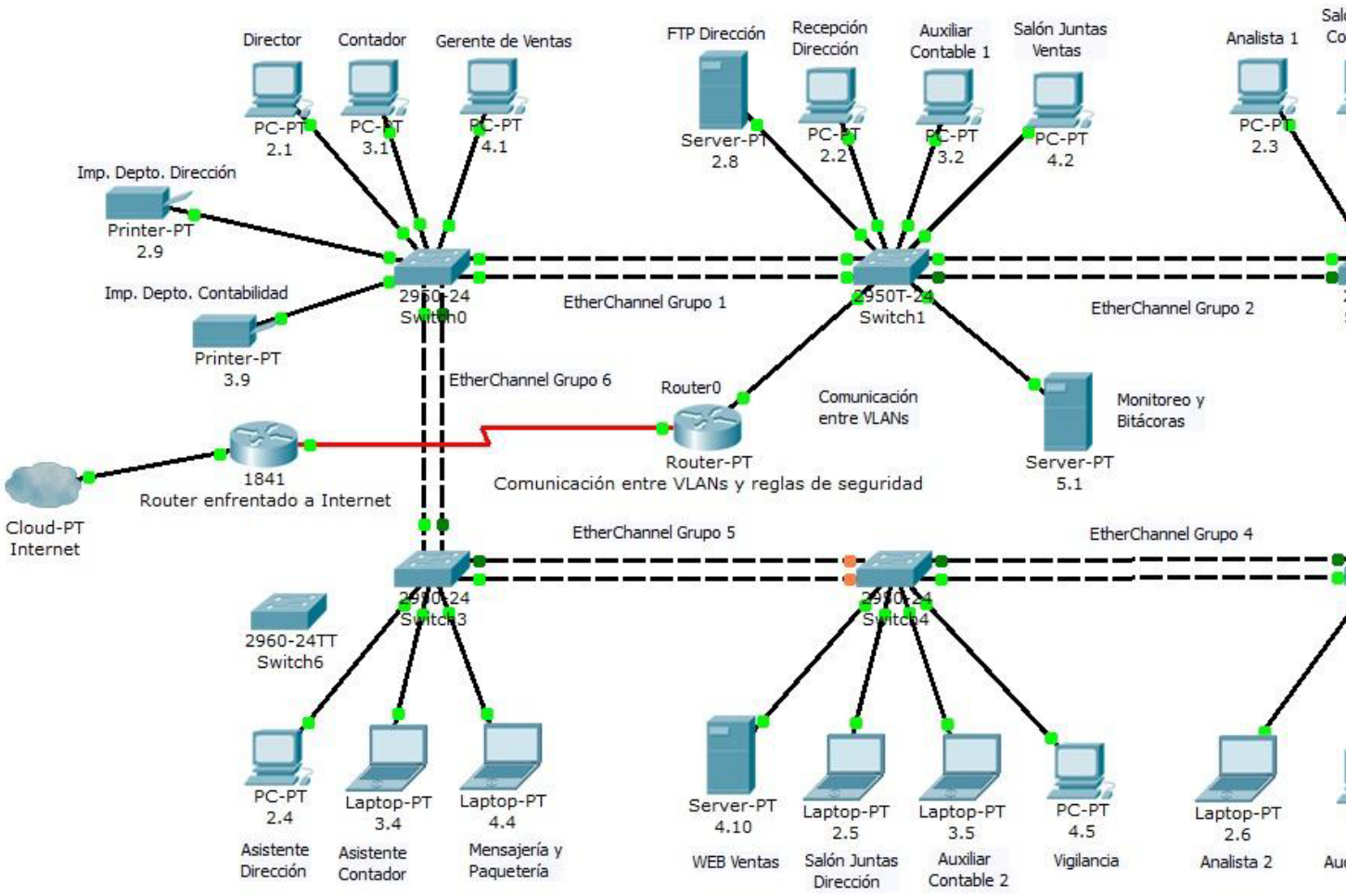
- Este proyecto se acompaña de un archivo que contiene la simulación en el software Packet Tracer de Cisco versión 5.2, donde se muestra la simulación y configuración completa de este Proyecto Terminal. En la siguiente sección se incluye una imagen de la simulación.
- Antes de comenzar con la configuración, se tiene que instalar previamente todo el cableado estructurado (UTP Cat5) en los edificios correspondientes, el equipo implicado como racks, switches, routers, servidores, impresoras y PCs, etc., en su ubicación final (con excepción de las Laptops); además, el software y aplicaciones necesarias en las PCs.
- Para efecto de la configuración de este Proyecto Terminal, los comandos se aplican de la misma forma en los switches Catalyst serie 2960 y Catalyst serie 2950. La ilustración de la simulación, es sólo para la comprensión del funcionamiento de las VLANs, sin embargo, puede tener otro arreglo físico, sin afectar su configuración y operatividad.
- Las Pcs pueden tener instalado cualquier Sistema Operativo (Windows, Linux, Mac OS), en cada caso se tendrá que configurar la dirección IP y la máscara de red de manera estática.
- Cada computadora debe tener correctamente configurada y habilitada su interfaz Ethernet. Los servidores al igual que las impresoras de la red deben de configurarse previamente a la instalación de la misma, es decir, tienen que estar listos para incorporarse a ella.
- Se utilizó una Laptop para la configuración de los equipos de comunicación y un cable RJ-45 a Serial. Se copia el texto tal y como se configura en la terminal de los dispositivos, se agregan unos espacios para una mejor visualización de los mensajes que arroja la terminal.
- Los comandos de configuración aparecen con texto en negrita en la siguiente sección. No importan el orden en que se configuren los

dispositivos, siempre y cuando todo estén completamente configurados, lo anterior aplica también para las los dispositivos terminales y servidores.

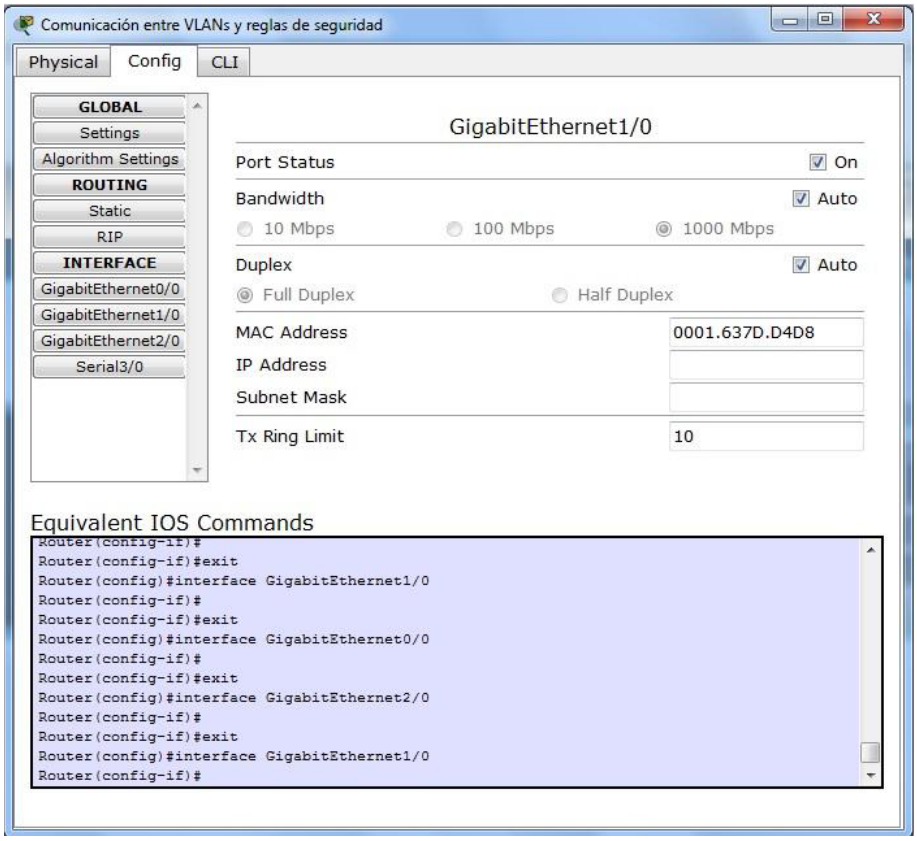
- La instalación física del cableado, dispositivos de comunicación, equipos terminales; instalación y configuración de los Sistemas Operativos, tarjetas Ethernet, aplicaciones, conexión de impresoras directamente a la red y servidores; quedan fuera del alcance de este Proyecto Terminal, ya que sólo se concentra en el diseño e implantación de la red.
- El texto de color azul son comentarios que explican lo que se configurará a continuación.
- El texto de color negro que comienza con un "%", son mensajes que arroja el Sistema Operativo de los dispositivos de red (IOS, *Internetwork Operating System*) al ejecutar una instrucción.
- Los puntos verdes en la simulación, significa que hay comunicación en capa 1, la configuración de las VLANs y reglas de seguridad, se realiza en la CLI *(Command Line Interface*) de cada dispositivo.
- Nótese que además de haber redundancia, están encendidos (color verde) ambos enlaces entre switches, esto es por efecto del *EtherChannel*, sin embargo, en el grupo 5, hay dos puntos de color ámbar, esto indica que **no** hay comunicación a través de esos enlaces, esto es resultado del *Spanning-Tree Protocol*, lo cual es correcto.
- Finalmente, existen otras reglas de seguridad muy interesantes y sobre todo útiles en la aplicación de las redes de computadoras en la industria, se conocen como Listas de Control de Acceso (ACLs, *Access Control Lists*), sin embargo, esa es otra historia.

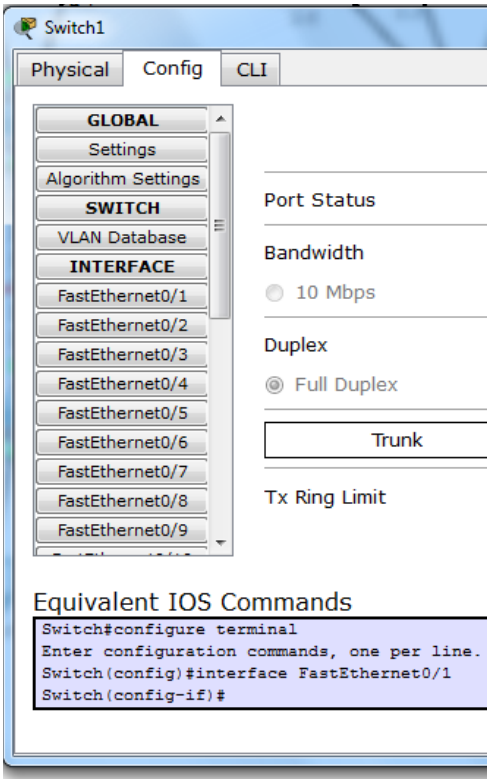
Imágenes del Proyecto Terminal en el Simulador Packet Tracer

Número de VLAN	Nombre	Segmer
1	Default	192.1
2	Dirección	192.1
3	Contabilidad	192.1
4	Ventas	192.1
5	AdmonRed	192.1



Interfaz gráfica para la configuración de los puertos del Router0





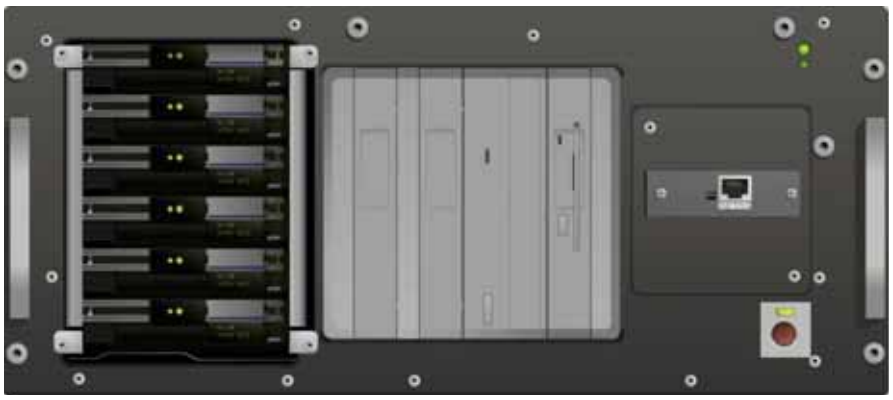
Interfaz grá
configurac
puertos d

Imágenes (aproximadas) de los dispositivo

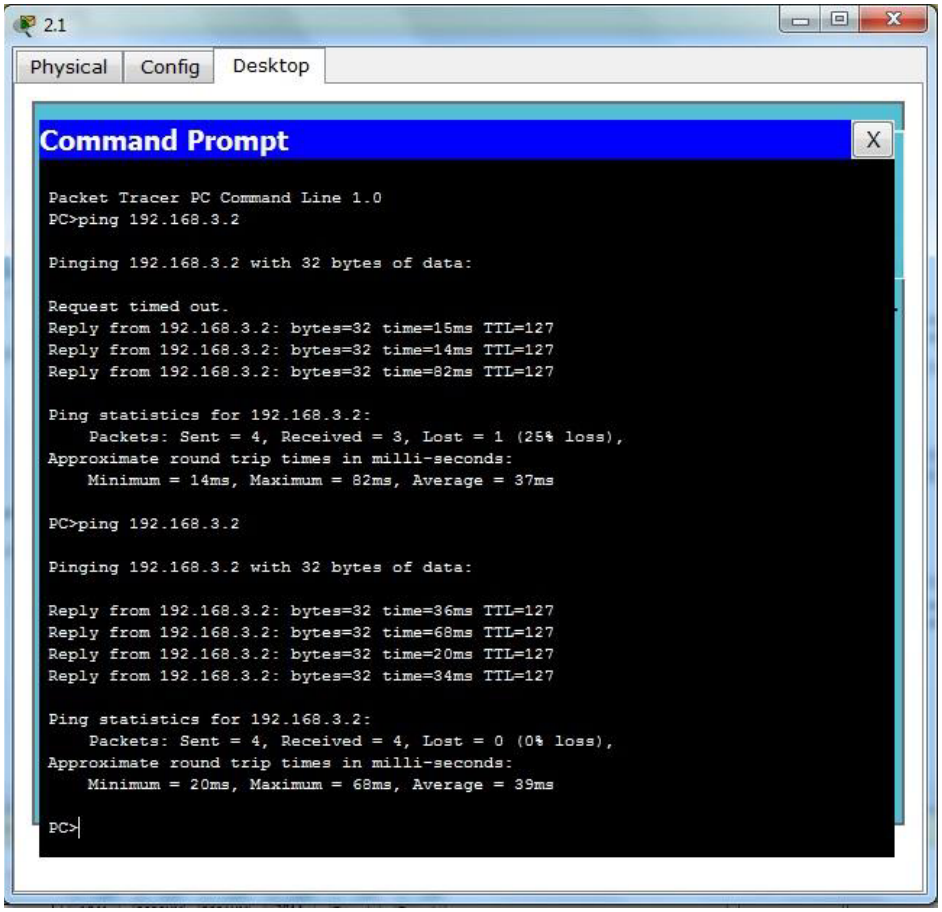
Imagen del switch Catalyst 2960

Imagen del router 1841

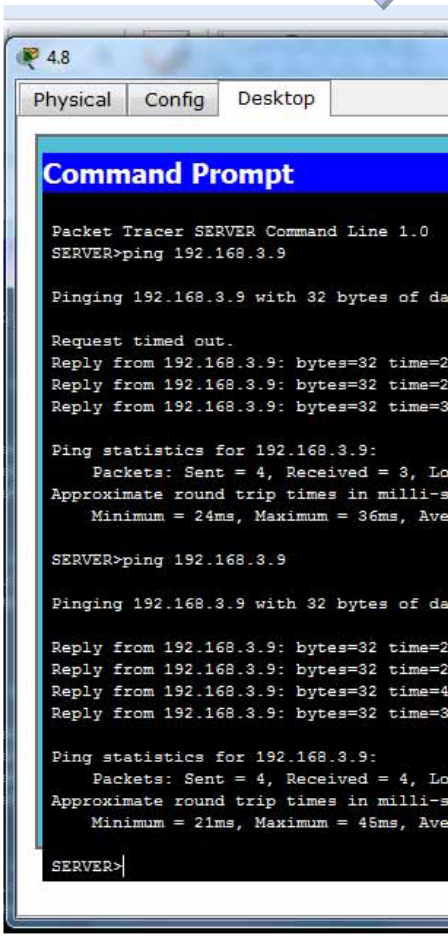
Imagen de un servidor genérico



Ventana que muestra la comunicación de la computadora del Director con la del Auxiliar Contable I



Ventana que muestra la
Servidor FTP Ventas con
Departamento de C



13.1 Configuración de los dispositivos

Switches Cisco Catalyst 2960

- **Configuración del Switch0**

Activamos el switch y entramos al modo de configuración global.

Switch>**enable**
Switch#**configure terminal**

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

Switch(config)#

Creamos las VLANs y les asignamos su respectivo nombre.

Switch(config)#**vlan 2**
Switch(config-vlan)#**name Direccion**
Switch(config-vlan)#**exit**
Switch(config)#**vlan 3**
Switch(config-vlan)#**name Contabilidad**
Switch(config-vlan)#**exit**
Switch(config)#**vlan 4**
Switch(config-vlan)#**name Ventas**
Switch(config-vlan)#**exit**
Switch(config)#

Encendemos los puertos y los asignamos a sus VLANs correspondientes. En cada puerto conectado a un dispositivo terminal configuramos Port-Fast, BPDU Guard y Port Security modo sticky.

Switch(config)#**interface FastEthernet 0/05**
Switch(config-if)#**no shutdown**
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan 2**
Switch(config-if)#**spanning-tree portfast**

%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Portfast has been configured on FastEthernet0/5 but will only
have effect when the interface is in a non-trunking mode.

Switch(config-if)#**spanning-tree bpduguard enable**
Switch(config-if)#**switchport port-security mac-address sticky**
Switch(config-if)#**exit**
Switch(config)#**interface FastEthernet 0/06**

Switch(config-if)#**no shutdown**
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan 3**
Switch(config-if)#**spanning-tree portfast**

%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/6 but will only
have effect when the interface is in a non-trunking mode.

Switch(config-if)#**spanning-tree bpduguard enable**
Switch(config-if)#**switchport port-security mac-address sticky**
Switch(config-if)#**exit**
Switch(config)#**interface FastEthernet 0/07**
Switch(config-if)#**no shutdown**
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan 4**
Switch(config-if)#**spanning-tree portfast**

%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Portfast has been configured on FastEthernet0/7 but will only
have effect when the interface is in a non-trunking mode.

Switch(config-if)#**spanning-tree bpduguard enable**
Switch(config-if)#**switchport port-security mac-address sticky**
Switch(config-if)#**exit**
Switch(config)#**interface FastEthernet 0/08**
Switch(config-if)#**no shutdown**
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan 2**
Switch(config-if)#**spanning-tree portfast**

%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Portfast has been configured on FastEthernet0/8 but will only
have effect when the interface is in a non-trunking mode.
Switch(config-if)#**spanning-tree bpduguard enable**

Switch(config-if)#**switchport port-security mac-address sticky**
Switch(config-if)#**exit**
Switch(config)#**interface FastEthernet 0/09**
Switch(config-if)#**no shutdown**

Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan 3**
Switch(config-if)#**spanning-tree portfast**

%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Portfast has been configured on FastEthernet0/9 but will only

have effect when the interface is in a non-trunking mode.
Switch(config-if)#**spanning-tree bpduguard enable**
Switch(config-if)#**switchport port-security mac-address sticky**
Switch(config-if)#**exit**

Configuramos los enlaces troncales aplicando EtherChannel asignados a su respectivo grupo.

Switch(config)#**interface range FastEthernet 0/01-4**
Switch(config-if)#**no shutdown**
Switch(config-if-range)#**switchport mode trunk**

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed
state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed
state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed
state to up

Switch(config-if-range)#**exit**
Switch(config)#**interface range FastEthernet 0/01-2**
Switch(config-if-range)#**channel-group 1 mode on**

%LINK-5-CHANGED: Interface Port-channel 1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel 1, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

Switch(config-if-range)#**exit**
Switch(config)#**interface Range Fastethernet 0/03-4**
Switch(config-if-range)#**channel-group 6 mode on**

%LINK-5-CHANGED: Interface Port-channel 6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel 6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to upSwitch(config-if-range)#**exit**

Switch(config)#**exit**
Switch#

%SYS-5-CONFIG_I: Configured from console by console
Switch#**copy run start**

Destination filename [startup-config]?
Building configuration...
[OK]

Switch# [*Configuración finalizada Switch0*]

Por simplicidad se omiten las explicaciones similares de la configuración del switch0 para el resto de los switches, a excepción de que se utilicen nuevos comandos.

- **Configuración del Switch1**

Switch>**enable**
Switch#**configure terminal**

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

Switch(config)#**vlan 2**

Switch(config-vlan)#**name Direccion**
Switch(config-vlan)#**exit**
Switch(config)#**vlan 3**
Switch(config-vlan)#**name Contabilidad**
Switch(config-vlan)#**exit**
Switch(config)#**vlan 4**
Switch(config-vlan)#**name Ventas**
Switch(config-vlan)#**exit**

Se agrega la VLAN 5 para el servidor de Monitoreo y Bitácoras.

Switch(config)#**vlan 5**
Switch(config-vlan)#**name AdmonRed**
Switch(config-vlan)#**exit**

continuamos…

Switch(config)#**interface FastEthernet 0/05**
Switch(config-if)#**no shutdown**
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan 2**
Switch(config-if)#**spanning-tree portfast**

%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/5 but will only
have effect when the interface is in a non-trunking mode.

Switch(config-if)#**spanning-tree bpduguard enable**
Switch(config-if)#**switchport port-security mac-address sticky**
Switch(config-if)#**exit**
Switch(config)#**interface FastEthernet 0/06**
Switch(config-if)#**no shutdown**
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan 3**
Switch(config-if)#**spanning-tree portfast**

%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/6 but will only
have effect when the interface is in a non-trunking mode.

Switch(config-if)#**spanning-tree bpduguard enable**
Switch(config-if)#**switchport port-security mac-address sticky**

Switch(config-if)#**exit**
Switch(config)#**interface FastEthernet 0/07**
Switch(config-if)#**no shutdown**
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan 4**
Switch(config-if)#**spanning-tree portfast**

%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Portfast has been configured on FastEthernet0/7 but will only
have effect when the interface is in a non-trunking mode.

Switch(config-if)#**spanning-tree bpduguard enable**
Switch(config-if)#**switchport port-security mac-address sticky**
Switch(config-if)#**exit**

Se agrega el puerto FastEthernet 0/8 correspondiente al servidor FTP del Depto. de Dirección a la VLAN2.

Switch(config)#**interface FastEthernet 0/08**
Switch(config-if)#**no shutdown**
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan 2**
Switch(config-if)#**spanning-tree portfast**

%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Portfast has been configured on FastEthernet0/8 but will only
have effect when the interface is in a non-trunking mode.

Switch(config-if)#**spanning-tree bpduguard enable**
Switch(config-if)#**switchport port-security mac-address sticky**
Switch(config-if)#**exit**

Se agrega el puerto FastEthernet 0/9 correspondiente al servidor de Monitoreo y Bitácoras a la VLAN 5.

Switch(config)#**interface FastEthernet 0/09**
Switch(config-if)#**no shutdown**
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan 5**
Switch(config-if)#**spanning-tree portfast**

%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this

interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Portfast has been configured on FastEthernet0/9 but will only
have effect when the interface is in a non-trunking mode.
Switch(config-if)#**spanning-tree bpduguard enable**
Switch(config-if)#**switchport port-security mac-address sticky**
Switch(config-if)#**exit**
Switch(config)#

Configuramos el puerto GigabitEthernet_1 como troncal ya que está conectado al router que permite la comunicación entre VLANs.

Switch(config)#**interface GigabitEthernet 1/1**
Switch(config-if)#**no shutdown**
Switch(config-if)#**switchport mode trunk**
Switch(config-if)#**exit**

continuamos…

Switch(config)#**interface range FastEthernet 0/01-4**
Switch(config-if-range)#**no shutdown**
Switch(config-if-range)#**switchport mode trunk**

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

Switch(config-if-range)#**exit**
Switch(config)#**interface range FastEthernet 0/1-2**
Switch(config-if-range)#**channel-group 1 mode on**

%LINK-5-CHANGED: Interface Port-channel 1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel 1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

Switch(config-if-range)#**exit**

Switch(config)#**interface range FastEthernet 0/3-4**
Switch(config-if-range)#**channel-group 2 mode on**

%LINK-5-CHANGED: Interface Port-channel 2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel 2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

Switch(config-if-range)#**exit**

*Configuramos este switch para que sea **root** en el Protocolo Árbol de Extensión (STP) de todas las VLANs.*

Switch(config)#**spanning-tree vlan 2 root primary**
Switch(config)#**spanning-tree vlan 3 root primary**
Switch(config)#**spanning-tree vlan 4 root primary**
Switch(config)#**spanning-tree vlan 5 root primary**
Switch(config)#

continuamos…

Switch(config)#**exit**
Switch#

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

Switch#**copy run start**

Destination filename [startup-config]?
Building configuration...
[OK]

Switch# [*Configuración finalizada Switch1*]

Nota

La configuración del switch2, switch3, switch4, switch5, es similar a las anteriores.

Router Cisco 1800 Series Integrated Service (1841)

- **Configuración del Router0**

*El comando **encapsulation dot1q**… se refiera a que se utilizará el protocolo de encapsulado para redes Ethernet conocido como el estándar 802.1Q. Esta configuración permitirá la comunicación entre VLANs.*

Router>**enable**
Router#**configure terminal**

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

Router(config)#**interface GigabitEthernet 1/0**
Router(config-if)#**no shutdown**

%LINK-5-CHANGED: Interface GigabitEthernet1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up

Router(config-if)#**exit**
Router(config)#**interface GigabitEthernet 1/0.2**

%LINK-5-CHANGED: Interface GigabitEthernet1/0.2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0.2, changed state to up

Router(config-subif)#**encapsulation dot1q 2**
Router(config-subif)#**ip address 192.168.2.7 255.255.255.0**
Router(config-subif)#**no shutdown**
Router(config-subif)#**exit**
Router(config)#**interface GigabitEthernet 1/0.3**

%LINK-5-CHANGED: Interface GigabitEthernet1/0.3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0.3, changed state to up

Router(config-subif)#**encapsulation dot1q 3**
Router(config-subif)#**ip address 192.168.3.7 255.255.255.0**
Router(config-subif)#**no shutdown**
Router(config-subif)#**exit**
Router(config)#**interface GigabitEthernet 1/0.4**

%LINK-5-CHANGED: Interface GigabitEthernet1/0.4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0.4, changed state to up
Router(config-subif)#**encapsulation dot1q 4**
Router(config-subif)#**ip address 192.168.4.7 255.255.255.0**
Router(config-subif)#**no shutdown**

Router(config-subif)#**exit**
Router(config)#**interface GigabitEthernet 1/0.5**

%LINK-5-CHANGED: Interface GigabitEthernet1/0.5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0.5, changed state to up

Router(config-subif)#**encapsulation dot1q 5**
Router(config-subif)#**ip address 192.168.5.7 255.255.255.0**
Router(config-subif)#**no shutdown**
Router(config-subif)#**exit**
Router(config)#**exit**

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

Router# [*Configuración finalizada Router0*]

15. Bibliografía y Cibergrafía

Disponibilidad verificada al 24 de Agosto de 2010.

Capítulos 2 y 3.

- Charles Babbage:
http://www.sciencemuseum.org.uk/onlinestuff/stories/babbage.aspx
http://projects.exeter.ac.uk/babbage/biograph.html

- Ada Agusta Byron:
http://www.sciencemuseum.org.uk/onlinestuff/stories/ada_lovelace.aspx
http://www.agnesscott.edu/lriddle/women/love.htm

- George Boole
http://www.kerryr.net/pioneers/boole.htm
http://plato.stanford.edu/entries/boole/

- Hermann Hollerith
http://www.hermanhollerith.com.ar/BiografiaHH.shtm
http://www-03.ibm.com/ibm/history/exhibits/builders/builders_hollerith.html

- Alan Mathison Turing
http://www.turing.org.uk/turing/index.html
http://www.alanturing.net/turing_archive/index.html

- Konrad Suze
http://ei.cs.vt.edu/~history/Zuse.html
http://user.cs.tu-berlin.de/~zuse/Konrad_Zuse/index.html

- Howard H. Aiken
http://www.thocp.net/biographies/aiken_howard.html
http://www-history.mcs.st-andrews.ac.uk/Biographies/Aiken.html

- John von Neumann
http://ei.cs.vt.edu/~history/VonNeumann.html
http://www-history.mcs.st-andrews.ac.uk/Biographies/Von_Neumann.html

- Robert Taylor
http://enc.slider.com/Enc/Robert_Taylor_%28computer_scientist%29
http://www.rheingold.com/texts/tft/10.html

- Douglas Engelbart
http://www.dougengelbart.org/about/dce-bio.html
http://www.dougengelbart.org/about/cv.html

- Lawrence Roberts
http://www.packet.cc/
http://itsummit.kaust.edu.sa/bio-roberts.aspx

- J.R.C. Licklider
http://www.livinginternet.com/i/ii_licklider.htm
http://www.cbi.umn.edu/oh/display.phtml?id=87

- Leonard Kleinrock
http://www.lk.cs.ucla.edu/profile.html
http://www.lk.cs.ucla.edu/index.html

- Ivan Sutherland
http://www.cs.umd.edu/hcil/muiseum/sutherland/ivan_page.htm
http://web.mit.edu/invent/iow/sutherland.html

- Robert Khan
http://www.cnri.reston.va.us/bios/kahn.html
http://www.livinginternet.com/i/ii_kahn.htm

- Vinton Cerf
http://www.icann.org/en/biog/cerf.htm
http://www.ibiblio.org/pioneers/cerf.html

Capítulo 4.

- http://www.isoc.org/internet/history/brief.shtml#Origins
- http://www.computerhistory.org/internet_history/
- http://www.livinginternet.com/i/ii_arpanet.htm
- http://groups.csail.mit.edu/medg/people/psz/Licklider.html
- http://www.ziplink.net/~lroberts/InternetChronology.html
- http://www.newsroom.ucla.edu/portal/ucla/electronicplay.aspx?fid=28176&id=E0C5478

Capítulo 5.

- STALLINGS, William. Data and Computer Communications. 8 th. ed. Prentice Hall. 2007. 896 p.
- TANENBAUM, Andrew S. Computer Networks. 4 th. ed. Prentice Hall. 2003. 912 p.

Capítulos 6, 7, 8, y 9.

- http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Intro-to-Internet.html
- http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Intro-to-LAN.html
- http://www.cisco.com/en/US/docs/internetworking/technology/handbook/NM-Basics.html
- http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Ethernet.html
- http://www.cisco.com/en/US/docs/internetworking/technology/handbook/LAN-Switching.html
- http://www.cisco.com/en/US/docs/internetworking/technology/handbook/OSI-Protocols.html
- http://www.anixter.com/AXECOM/AXEDocLib.nsf/%28UnID%29/8F2E0839A6190F4986257309005757CC/$file/ANSI-TIA-EIA-568-B.pdf
- http://www.ertyu.org/steven_nikkel/ethernetcables.html

Capítulos 10, 11 y 12.

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/switch_c/xcvlan.htm
- http://net21.ucdavis.edu/newvlan.htm
- HUCABY, David y McQUERRY, Stephen. Cisco Field Manual: Catalyst Switch Configuration. 1 st. Cisco Press. 2003. 560 p.

Capítulo 13.

- http://www.cisco.com/en/US/tech/tk389/tk689/technologies_configuration_example09186a008009478e.shtml
- http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_55_se/configuration/guide/2960scg.pdf
- http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_55_se/command/reference/2960cr.pdf
- http://www.cisco.com/en/US/docs/routers/access/1800/1841/software/configuration/guide/b_cli.html