Universidad Nacional Autónoma de México

Facultad de Ingeniería

"Manual de Referencia Para Certificación Internacional en Redes"

T E S I S

Que para obtener el título de

Ingeniero en Computación

Presenta

Raúl Martínez Gómez

Asesora de Tesis

M.C. Ma. Jaquelina López Barrientos

México D.F. 2005

A Dios, a mi Preciosa Esposa y a mi Familia.

Índice

Panorama General

Una tendencia relativamente nueva pero que va tomando auge muy fuertemente hoy en día es la de certificar; cada vez es más necesario respaldar la palabra, los hechos, los resultados, etc. con una certificación; desde una certificación ante notario público de las bondades que ofrece un producto para adelgazar hasta, en la industria de la tecnología de la información, una certificación internacional. En el nuevo ambiente competitivo que se vive a escala mundial, no sólo es necesario poseer las habilidades y conocimientos requeridos para desarrollar una empresa, sino que es necesario además el garantizar bajo un estándar general que se cuenta con dichas habilidades y no solamente en la propia opinión sino en opinión de alguien o algún organismo reconocido como autoridad en la materia.

El panorama general detrás de una certificación internacional es sencillo pero con implicaciones en diversos ámbitos: a nivel personal, empresarial y, por supuesto, en el ámbito nacional.

Muchos estudiantes, al egresar de la universidad se enfrentan a la situación paradójica de encontrar un trabajo en donde aplicar sus conocimientos sin contar con experiencia laboral. Pareciera que se requiere tener experiencia para adquirir experiencia. Hay varias formas de romper ésta paradoja: entre las más comúnmente aceptadas está la de subemplearse en alguna empresa con la esperanza de que el teorema de Peter, que dice que "En una jerarquía, cada empleado tiende a ascender eventualmente hasta su nivel de incapacidad", sea una vez más probado correcto. La gran desventaja de este método es que si bien se adquiere experiencia, ésta no necesariamente será sobre los conocimientos adquiridos en la escuela, conocimientos que muchas veces van por delante de lo puesto en práctica en las empresas. No se debe olvidar, por otro lado, que es irresponsable tratar de cambiar algo sin entender con exactitud como es que funciona actualmente y que, finalmente, el aparente retroceso que se paga por adquirir experiencia es aceptable tanto para el empleado como para la empresa a fin de garantizar que el conocimiento dominado por el trabajador es adecuado para mantener la estabilidad ya lograda antes de proponer mejoras. En este mismo tenor, hay soluciones tales como trabajar como practicante o como becario por un periodo "razonable" en el que no se goza de los beneficios de ser trabajador (tales como un sueldo completo) sin embargo se tienen las responsabilidades de un trabajador normal. ¡Aún después del periodo de prueba existe la posibilidad de no ser contratado!

La certificación es una manera de proveer al individuo credenciales que garanticen el manejo efectivo y profesional de ciertos productos. En el caso concreto de las certificaciones en tecnologías de la información, éstas son avaladas por los fabricantes y desarrolladores de dichos productos a través de exámenes propios y a través de organismos creados por la propia industria como es el caso de la CompTIA (*The Computing Technology Industry Association.*) La CompTIA es una asociación no lucrativa y sin nexos comerciales que establece estándares a la comunidad tecnológica en las áreas de servicio de Internet, comercio electrónico, certificación técnica, desarrollo de recursos humanos, la mano de obra y entrenamiento y en general la industria de la computación en Estados Unidos, e integra los

requerimientos técnicos que los principales fabricantes de tecnología del mundo desean de los profesionales dedicados al manejo de sus productos. Bajo los estándares definidos por la CompTIA, los fabricantes más importantes del mundo desarrollan programas de certificación en el manejo especializado de sus productos.

Son entonces, las certificaciones en tecnologías de la información, programas desarrollados para demostrar que se poseen y se mantienen las habilidades relacionadas con *software* y *hardware* de fabricantes en particular, y son una medida importante del conocimiento y experiencia de un individuo en ese campo. Las certificaciones se otorgan a personas que demuestran su habilidad para realizar trabajos específicos e implementar soluciones con los productos de ciertos fabricantes. Esto provee una herramienta para definir objetiva, rápida y eficientemente las habilidades de trabajadores y candidatos bajo criterios estandarizados.

Los requerimientos para lograr una certificación internacional difieren para cada certificación y son específicos al fabricante, el producto y la función que se avala. Para convertirse en un profesional certificado es necesario aprobar exámenes rigurosos que son diseñados por profesionales en la industria y que prueban que el candidato es un experto, con preguntas que reflejan escenarios reales de trabajo.

El proceso de certificación se creó para demostrar las habilidades prácticas que se han obtenido con la experiencia en el campo laboral. Sin embargo, este mismo proceso es además una guía de las habilidades y conocimientos que una persona debe poseer para ser proficiente en una área determinada. Con esto en mente, una persona dispuesta y motivada puede adquirir o desarrollar las habilidades específicas para ser un experto certificado siguiendo la guía de lo que la industria considera más importante en cierta materia. Es importante no caer en la tentación de convertirse en un "tigre de papel" es decir, de buscar aprobar un examen de certificación como meta principal de la preparación para hacerlo, el candidato debe, más bien, convertirse en un experto real en los temas que el examen trata y por consecuencia aprobar dicho examen.

Varios exámenes de certificación son exámenes adaptivos, o sea que el tema y la dificultad de la pregunta que se presenta se basan no sólo en el temario del examen sino en la respuesta dada a la pregunta anterior. La intención detrás de este procedimiento es que para aprobar un examen adaptivo se deben dominar todos los temas en el temario y de una manera implícita también es darle un valor intrínseco a la certificación; Varios fabricantes presumen sus bajísimos índices de aprobación (en promedio alrededor del 20% de los candidatos que presentan un examen de certificación lo aprueban) pues con ello incrementan el valor y el nivel de la certificación y de sus profesionales certificados.

Obtener una certificación es un esfuerzo personal en el que el candidato se somete a un intenso programa de estudio y preparación para lograr beneficios para su carrera, conocimiento técnico especializado y, por supuesto, satisfacción personal.

La decisión de lograr una certificación puede ser difícil ya que representa un sacrificio en términos de tiempo y economía y al final pudiera no resultar ser el catalizador deseado. El "salto de fe" para perseguir una certificación normalmente se toma después de una profunda introspectiva y variadas opiniones de amigos y colegas. Un aspecto de interés en particular es cómo elegir entre una multitud de posibles certificaciones, ya que puede haber cierta confusión en cuanto a cuáles certificaciones ofrecen el mayor valor tanto de manera personal como para las empresas que contratan. La motivación para certificarse incluye factores emocionales así como el estado del mercado laboral actual.

En un estudio realizado en 2002 en 50 países a más de 8000 profesionales de la industria de la información por Thomson-Prometric[1], los principales motivantes para lograr una certificación, tanto para personas no certificadas como para las ya certificadas incluyen: incrementar la credibilidad, poseer habilidades y conocimiento, incrementar compensaciones, aumentar productividad, mantenerse al día con nueva tecnología, satisfacer requerimientos del trabajo actual, ayudarse a conseguir empleo, prepararse para un nuevo puesto y cambiar de trabajo. Véase tabla I.

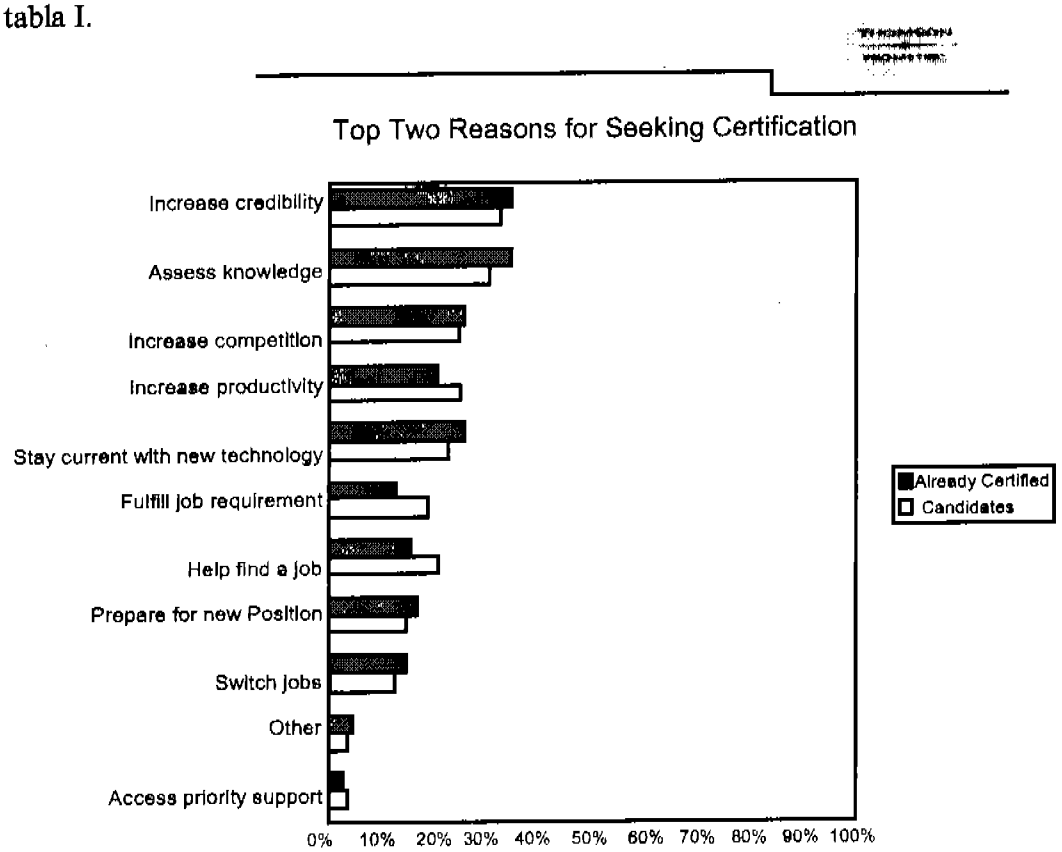


Tabla I. Razones para Buscar una certificación.

[1] www.prometrics.com

El mismo estudio reflejó que los principales beneficios para obtener una certificación incluyen: elevar la auto-confianza, acelerar el crecimiento profesional y mantenerse al día con nuevas tecnologías. Véase la tabla II.

Key Benefits of Certification	%Agree/Strongly Agree	
	Candidate	Already Certified
Certification is a great achievement- the result of hard work and personal sacrifice	78%	84%
Certification boosts my self-confidence	78%	87%
I will speed up my profesional growth	73%	79%
I take technical training to stay up to date on new technology	73%	81%
Technical training gives me an opportunity to network with others in my field	70%	77%
Certification programs help me design a career path	69%	77%
Certification allows me to speak the "same language" with other IT professionals	67%	78%
Once certified, I feel I know the product well and can solve problems faster	67%	77%

Tabla II. Beneficios de la certificación.

Existen diferencias importantes para diversos países y regiones en cuanto a la utilidad de una certificación. Por ejemplo, en China la principal razón para obtenerla es el incrementar la productividad, mientras que en India es conseguir un empleo, en Asia es el obtener conocimiento y en América Latina es el tener una mayor credibilidad. Ver la tabla III.

Top Two Reasons that Candidates Seek Certification by Geographic Location [%]									
	North America	Europe	Latin America	Africa/ Middle East	Asia/ Pacific	U.K./ Ireland	China	India	Other
Increase Productivity	11	12	12	16	20	7	33	22	12
Prepare for new position	7	10	9	9	6	6	10	12	10
Switch jobs	7	3	6	12	4	9	4	7	8
Help find a job	19	6	9	12	6	10	10	22	15
Increase compensation	8	8	6	5	7	7	8	1	5
Increase credibility	16	19	36	9	11	23	2	9	23
Fulfill job requirment	11	11	6	7	8	7	12	6	13
Assess knowledge	10	19	12	16	25	16	12	14	8
Stay current with new technology	10	8	0	9	8	14	4	5	5
Access vendor support	0	4	0	5	3	0	4	1	0
Other	2	1	3	0	2	2	2	0	2

Tabla III. Certificaciones por locación geográfica.

Los candidatos en India son más positivos en general en cuanto a los beneficios de obtener una certificación. Ellos están significativamente más de acuerdo en que al obtener una certificación internacional reciben reconocimiento en su trabajo actual y tienen la oportunidad de trabajar en cualquier lugar del mundo. Además el ser certificados les ayuda a avanzar hacia posiciones de mayor jerarquía y finalmente les resulta en una mejor calidad de vida para ellos y sus familias. Es impactante saber que el principal exportador de recursos humanos en el área de tecnología de la información es India.

Es bastante claro, en general, que los trabajadores jóvenes perciben la certificación más como una herramienta de avance y esperan más los beneficios "añadidos" como pueden ser influenciar positivamente a aquellos que en cierto modo tienen control sobre sus carreras (empleadores, colegas, jefes, clientes.) Sin embargo, los candidatos menores a los 30 años son menos atraídos a seguir adelante en su búsqueda de una certificación, principalmente debido a su economía.

En México, varios fabricantes ofrecen programas de entrenamiento para lograr la certificación en sus productos a costos poco menores que prohibitivos, por ejemplo Microsoft ofrece a través de centros de entrenamiento técnico, la oportunidad de tomar cursos que eventualmente llevaran al estudiante a la certificación pero no hay una relación directa curso-examen de certificación por lo que el alumno debe tomar varios cursos para presentar un solo examen de certificación para el cual habrá material que domina y no es tema del examen así como material que necesita para el examen y no tuvo la oportunidad de aprender en el curso de capacitación.

La implicación de esto es que a pesar del alto valor que se le da a una certificación como medio de superación y de avance en la carrera, hay un punto en el que el costo del entrenamiento y preparación es mayor que el posible beneficio a futuro para algunos.

Objetivo del Trabajo

El objetivo de este trabajo es el de proveer una herramienta importante para que las personas correctamente motivadas logren obtener una de las certificaciones más buscadas y reconocidas por la industria, la de CCNA de Cisco, de una manera flexible y económica.

Es importante notar en la tabla II en la sección de panorama general que el principal beneficio al lograr una certificación internacional es el incremento en la confianza en uno mismo. El ser un profesional certificado tiene que ver más con la excelencia que con la remuneración que el ser excelente en un área conlleve. Desde luego que las expectativas que se tengan y los motivos para conseguir una certificación determinarán el grado de satisfacción o, en su caso, de desilusión al recibir los beneficios de ésta. La definición personal de "éxito" debe ser tomada en cuenta antes de iniciar el camino en pos de una certificación. Hay una sutil diferencia entre certificarse para lograr obtener un buen empleo y obtener un buen trabajo gracias a que se está certificado, sin embargo, es una diferencia de raíz que tiene que ver con el por qué.

Un día, en su lugar de retiro en Maine, el célebre escritor Henry David Thoreau, notó un grupo de obreros que interrumpían su descanso. Al investigar, descubrió que estaban colocando una serie de alambres que formaban parte de un novedoso invento llamado telégrafo. ¡Han inventado el telégrafo! ¡Ahora, la gente en Florida puede comunicarse instantáneamente con la gente en Maine! -¡Que maravilloso! ... ¿pero que pasa si la gente en Florida no tiene nada que decir a la gente en Maine?

Los estándares definidos por las empresas de qué conocimientos y habilidades son más apreciadas se basan por supuesto en las necesidades reales de la industria y el valor de una certificación u otra se define en la mayor o menor utilidad de ellas en el ámbito real, de modo que el candidato a una certificación debe de ver más allá de la consecución de sus propias satisfacciones y pensar en convertirse en la persona más útil que puede ser, tomando una frase popularizada por el ejército, "Sé todo lo que puedes ser" y es claro que para ser todo lo que se puede ser, es necesario considerar a fondo quién se es. Lo anterior pudiera parecer obvio pero muchas veces es pasado por alto al considerar otros factores de motivación como la estabilidad financiera y el reconocimiento personal.

En resumen, una certificación puede ser un catalizador en la carrera y puede proyectar los ingresos personales y el reconocimiento a niveles que de otro modo se alcanzan mucho más paulatinamente. Sin embargo, un análisis profundo debe mostrar que las razones para perseguir este logro son internas más que externas, para no acabar siendo lo que alguien más quiere que se sea (inclusive si ese alguien es Microsoft o Cisco) sino para ser la mejor persona que se puede ser.

Una creencia general es que el valor de las certificaciones puede disminuir si demasiadas personas las poseen, personalmente pienso que no es posible tener "demasiadas" personas de excelencia. India, la primer potencia mundial en

desarrolladores de *software*, es un ejemplo claro de que la excelencia personal en cierta área eventualmente se reflejará en la excelencia nacional.

Una certificación es una herramienta muy poderosa y como tal puede ser utilizada correcta o incorrectamente por lo que obtenerla no debe ser el fin principal de obtenerla, el objetivo del conocimiento es usarlo. Desde luego que el trabajo plenamente gratificante es el más deseado, pero se nos ha enseñado que, desafortunadamente, también es muy raro. Los trabajos que proveen un éxtasis psicológico no son fáciles de encontrar, pero aún aquellos trabajos que parecen ser los más encantadores conllevan una serie de tareas desagradables y sacrificios.

El trabajo ideal no es el mismo para todos y cuanto antes se determinen las metas personales de manera profunda se evitara el peligro de utilizar la certificación como una forma rápida de llegar... a donde no se quería ir. La certificación es una herramienta para el contentamiento, no se confunda con el conformismo ya que la excelencia requiere de mayores sacrificios que la mera persecución de beneficios.

Una de las certificaciones más buscadas por la industria en los últimos años es la de CCNA (*Cisco Certified Network Associate.*) En 2002, ésta certificación fue la más popular según una encuesta realizada por Becky Nagel para Certcities[1] para otorgar el premio "*Readers Choice Award*". El año siguiente, CCNA de Cisco fue votada la segunda certificación más buscada por la industria al contratar a sus profesionales, además fue finalista como la mejor certificación de primer nivel a poseer a escala mundial, (el título se lo llevó la certificación A+ de CompTIA) mientras que Cisco obtuvo el título general más importante por "El Mejor Programa de Certificaciones en el Mundo"

Una certificación Cisco concede al poseedor un entendimiento profundo de la interrelación de redes computacionales no solamente de productos Cisco; para obtenerla es necesario entender cómo distintas topologías, medios, protocolos y dispositivos trabajan en conjunto para formar una red. Esto es benéfico para cualquier red y es la principal razón de la gran demanda que gozan las certificaciones Cisco, aún en compañías con pocos dispositivos Cisco.

Cisco divide sus certificaciones en tres niveles: asociado, profesional y experto (Véase la figura I.)

En la base de la pirámide se encuentran las certificaciones CCNA (*Cisco Certified Network Associate*) y CCDA (*Cisco Certified Design Associate.*)

CCNA provee una fundación sólida para entender el sistema operativo de redes Cisco (IOS) y el *hardware* Cisco, además de las interconexiones de redes en general, necesarias para planear, instalar, configurar y mantener redes LAN y WAN.

[1] www.certcities.com

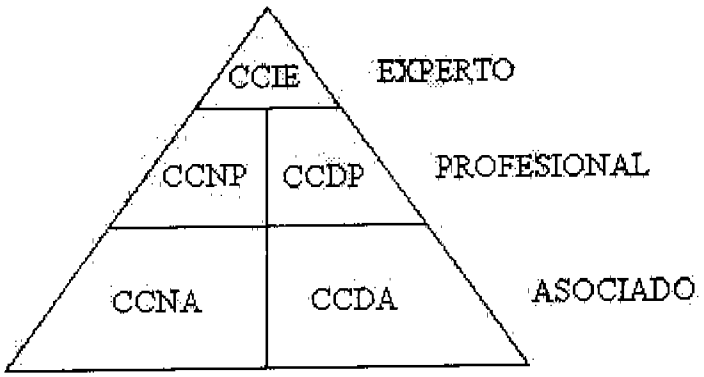


Figura I Niveles de certificación Cisco

Para subir al siguiente nivel tan solo es necesario aprobar una de las dos certificaciones en la base.

En el siguiente nivel se encuentra la certificación CCNP (*Cisco Certified Network Professional*), para tomar este examen es necesario contar con la certificación CCNA del nivel anterior. Un CCNP está preparado para resolver problemas complejos de interconexión de redes actuales y de tecnologías nacientes además de dominar las habilidades necesarias para ser CCNA.

En la cima de la pirámide se encuentra la certificación más robusta existente en cuanto al manejo de redes, y es curioso que para presentar el examen de certificación CCIE (*Cisco Certified Internetworking Expert*) no es requisito tener ninguna otra certificación. El examen se divide en dos partes, una escrita con duración de 75 minutos (actualmente cuesta $300 USD) y un laboratorio de un día entero en un ambiente controlado en las instalaciones de Cisco, la gran mayoría de los candidatos reprueba este examen en su primer ¡y segundo! Intentos, es un laboratorio sumamente difícil (y actualmente cuesta $1250 USD), algunas personas simplemente nunca lo pueden aprobar.

Sobre la ruta de diseño se encuentran en el primer nivel el CCDA y en el nivel profesional el CCDP. Estas certificaciones no son tan profundas en lo técnico o exigentes como sus contrapartes por nivel ya que se concentran en aspectos de planeación y diseño como son el tamaño, filtrado, división, etc. de una red. Sin embargo, para lograrlas se recomienda poseer los conocimientos equivalentes o las certificaciones CCNA o CCNP según el caso.

Cisco es la compañía más importante del mundo en materia de ruteo y *switcheo*, el Microsoft del mundo de las redes. El buscar una certificación Cisco es buscar ser el mejor, el mejor en ruteo y el mejor en *switcheo*. El objetivo particular de este trabajo es dar una guía accesible para tomar el primer paso en esa dirección: convertirse en un CCNA.

Metodología

La manera de convertirse en un profesional certificado CCNA es simplemente pasar un examen; el examen 640-801 de Cisco. Sin embargo, para aprobar este examen adaptivo de 90 minutos es necesario poseer una gran cantidad de conocimientos y tener la capacidad de distinguir las implicaciones de pequeñas variaciones en diferentes escenarios. Hace algunos años, las únicas personas capaces de presentar dicho examen eran profesionales dedicados al campo de las redes ruteadas con experiencia de varios años, y aún de entre estos candidatos pocos podían hacerlo solventemente.

Actualmente, existen numerosas ayudas para que el profesional que ya cuenta con experiencia pueda afinar sus conocimientos hacia los requerimientos del examen. Una de las herramientas más comúnmente utilizadas son los "*Boot Camps*" o campamentos de booteo. Un campo de booteo es una especie de retiro en el que el candidato se aparta del mundo para dedicarse única y exclusivamente a la consecución de un logro: Aprobar el examen 640-801. En estos campos (tal vez sería mejor llamarlos acuartelamientos), el "campero" tiene extensas sesiones de capacitación teórica y muchas oportunidades de poner en práctica lo recién discutido en ambientes ex profeso diseñados para ilustrar los conceptos tratados en la parte teórica. La duración de un boot camp es normalmente de 3 a 5 días y concluye con la aplicación del examen.

Hay un algunos inconvenientes en cuanto a este método de estudio: el primero es que son jornadas de estudio intensivo por varias horas diarias por pocos días, eso sugiere, y en la práctica se confirma ampliamente, que para asistir a un boot camp se necesita que el candidato ya sepa bastante del entorno de redes y que para alguien sin experiencia en el ámbito, resulta sumamente difícil seguir el paso de las pláticas y laboratorios y por ende entender los conceptos y ulteriormente aprobar el examen. Otro factor que para muchos aspirantes resulta decisivo es el costo; un boot camp para convertirse en CCNA tiene un costo de alrededor de $2000 USD (ver www.globalnettraining.com) más viáticos. La mayoría de las empresas que ofrecen campamentos de booteo piden además entre sus requisitos de inscripción el aprobar un examen de reclutamiento en el que se evalúa el manejo de los dispositivos. En otras palabras, que el candidato ya sepa hacer lo que va venir en el examen y solamente necesite saber porque lo hace así; la teoría que da soporte a lo que ya hace en la práctica.

Otro método para prepararse para presentar el examen consiste en estudiar guiado por un instructor o de manera independiente los temas que el examen cubre. Sin embargo, este método conlleva su intríngulis: Principalmente la dificultad de conseguir información confiable y específica. Existen manuales diseñados para cubrir esta necesidad, sin embargo estos manuales normalmente se encuentran en inglés y a miles de kilómetros de distancia y en mi experiencia como instructor de un centro de capacitación para certificaciones ninguno es adecuado a nuestras necesidades idiosincrásicas. Este trabajo pretende resolver ese problema proveyendo información concreta en español y para aspirantes mexicanos sobre los

temas que actualmente conforman el temario del examen, además de algunos que personalmente creo pudieran ser incluidos en el examen en un futuro.
A principios de 2004, Cisco anunció una vía alterna de exámenes para certificarse, en lugar de tomar el examen 640-801, ahora es posible tomar dos exámenes; El examen 640-821: *Introduction to Cisco Networking Technologies* (INTRO) y el examen 640-811: *Introduction to Cisco Networking Devices* (ICND.) Este manual facilita la consecución del primero de los dos exámenes, el examen CCNA-INTRO. La opción de dos exámenes es un poco más costosa pero podría resultar más fácil de seguir para algunas personas.

La metodología a seguir para lograr la certificación CCNA utilizando este manual es la siguiente:

- Revisar el temario para el examen a presentar. Los objetivos del examen están sujetos a cambios en cualquier momento y sin previo aviso, a discreción de Cisco. Esto se debe a que Cisco revisa constantemente los objetivos del examen para mantener la vigencia del mismo como garantía de satisfacción a las necesidades actuales y reales de la industria mundial y para considerar la integración de nuevas tecnologías en el examen. El temario se puede consultar en www.cisco.com/traincert.

- Comparar el temario actual del examen con el temario del manual. A pesar de que se incluyen temas pensando en cambios probables en los objetivos del examen, es factible que se hagan cambios no considerados en el manual. El desarrollo de los temas no incluidos en el manual se publicará a la brevedad posible, después de que Cisco anuncie la inclusión de un nuevo objetivo en el examen, en la siguiente dirección electrónica: www.raul.enpuebla.com.mx.

- Estudiar a conciencia los objetivos que comprende el examen a tomar. Aunque el presente manual es una herramienta sustancial para lograr la certificación, no debe ser tomado como la única herramienta necesaria. Es preciso que el estudiante lleve a la práctica los conocimientos adquiridos, para esto se sugieren ejercicios a lo largo del manual. Una buena alternativa para realizar muchos de los ejercicios recomendados es un simulador de ruteo (se toca el tema de los simuladores de ruteo en el capítulo 4.)

- Tomar exámenes de preparación. Una buena práctica es que el examen de certificación no sea el primer examen que se presente, existe una gran variedad de exámenes de preparación y con diferentes costos, incluyendo muchos gratuitos. Cisco da varias ligas a sitios de exámenes de preparación. En varias ciudades se puede acudir a algún centro de certificación para realizar un simulacro de examen con preguntas similares a las del examen real de manera gratuita.

- Consultar el temario publicado por Cisco nuevamente. El peor momento de enterarse que los objetivos del examen han cambiado es a medio examen.

- Agendar el examen. Hay más de 800 centros autorizados de certificación en el mundo. Para agendar el examen hay que determinar el centro en el que se quiere presentarlo. Para conocer el centro autorizado más cercano hay que visitar la página *Prometric Authorized Testing Centers* (www.2test.com) y la página de *Pearson VUE Authorized Centers* (www.vue.com), los centros listados en una página no necesariamente están listados en la otra. Al programar el examen se deberá cubrir el costo del mismo. Al momento de escribir este manual el costo del examen 640-801 es de $150 USD, el del examen 640-821 es de $75 USD y el del examen 640-811 es de $125 USD. Es posible programar el examen para el mismo día en que se quiere tomar o hasta seis semanas por anticipado, y es posible cancelarlo hasta 24 horas antes de la hora fijada para su inicio.

- Presentar el examen. El examen es adaptivo e incluye preguntas en varios formatos: opción múltiple de una o varias respuestas, arrastrar y soltar, completar enunciados y simulaciones de ruteo. Al momento, el porcentaje mínimo de aprobación es de 85%.

- ¡Incluir la nueva certificación en el currículo!

Capítulo 1

Fundamentos de redes

1.1 Introducción

Es innegable que la computación ha cambiado diametralmente desde sus inicios, y con las ciencias de la computación, las redes de computadoras. En este capítulo se hace una recapitulación de algunos de los conceptos básicos en el ámbito de las redes computacionales.

1.2 Concepto de Redes

Una red es, según el diccionario, un sistema en el que se conectan entre sí varios equipos independientes para compartir datos y periféricos. Por supuesto, existen varias definiciones más de lo que es una red ya que el concepto de red existe desde hace mucho tiempo y ha tomado muchos significados.

Según Cisco, las redes computacionales han existido desde que han existido las computadoras; el primer tipo de red que existió fue la red furtiva o *sneakernet*. Una red *sneakernet* realmente era una red más basada en las personas que en la tecnología. Tómese por ejemplo el siguiente caso, en cierta oficina un usuario quiere utilizar un recurso con el que no cuenta su computadora asignada, tal vez una impresora. Hay tres formas en las que este usuario puede imprimir su trabajo utilizando la *sneakernet* en otra computadora que cuente con el recurso: la primera es llevando su trabajo en un medio de almacenamiento extraíble, un disquete, a la computadora que tiene la impresora, la segunda es llevando la impresora a su propia computadora y la tercera es, por supuesto, haciendo su trabajo directamente en la computadora que cuenta con impresora. Esta es una *sneakernet*, una red furtiva o una red de alpargata. Véase la figura 1.1.

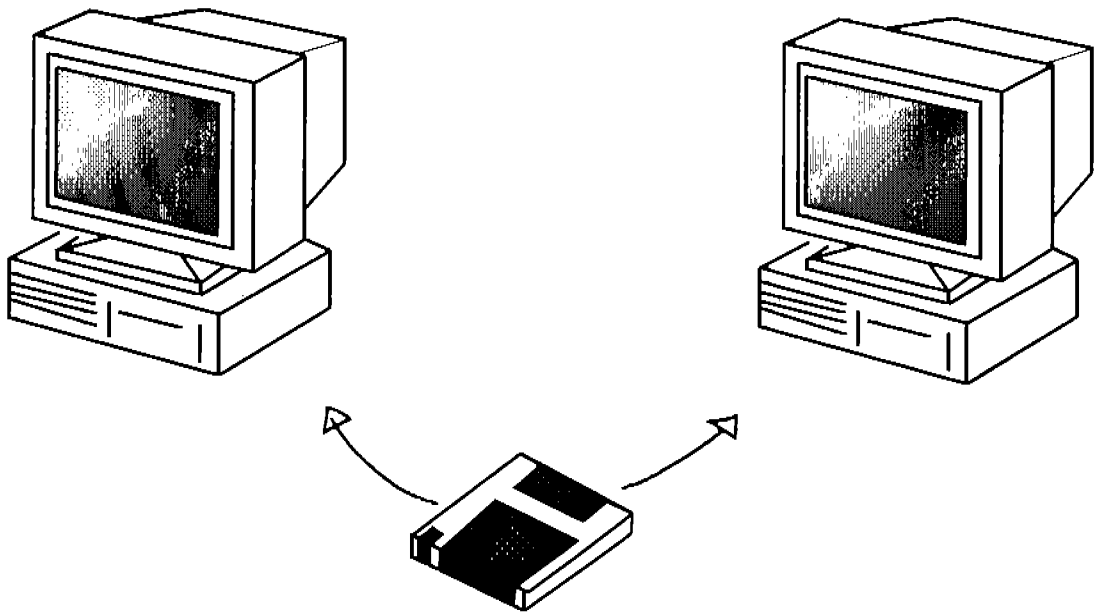


Figura 1.1 ***Sneakernet***

La red más elemental es la que se forma al unir dos equipos con un cable cruzado[1], por medio del cual comparten recursos. Las redes computacionales surgen como respuesta a la necesidad de compartir rápida y eficientemente recursos entre equipos. Cisco advierte que cualquier uso que se le dé a una red, caerá dentro de alguna de tres categorías:

- Compartir datos
- Compartir recursos de *software* y de *hardware*
- Centralizar la administración y soporte

El compartir información es uno de los usos más populares para las redes. Solo basta considerar los hábitos de uso de Internet de la gran mayoría de usuarios alrededor del mundo; Las principales actividades en Internet son el uso del correo electrónico y las conversaciones en línea.

La facilidad que dan las redes para compartir información hace que ésta se encuentre disponible simultáneamente a varios usuarios. Uno de los grandes ideales en el futuro de las redes que se planteó desde su inicio es llegar a tener "oficinas sin papel" y aunque esto se ve todavía muy distante, muestra sin duda el papel principal que las redes toman en el mundo cambiante de hoy. Actualmente, las redes computacionales son herramienta primordial para comunicarse rápida y eficazmente con grandes grupos de personas.

La segunda categoría que Cisco reconoce como una razón de la existencia de las redes es el poder compartir recursos de *software* y *hardware*. Antes de la aparición formal de las redes, los usuarios necesitaban tener sus propios recursos conectados a sus computadoras o atenerse a las incomodidades de una red furtiva. Ahora es posible que muchas computadoras compartan una sola impresora, un solo escáner, otros periféricos y hasta un mismo disco duro para almacenar su información. Asimismo, a través de una red es posible compartir aplicaciones con varios usuarios incluso de manera simultánea.

La tercera categoría dada por Cisco para el uso de una red es la administración centralizada y la facilidad de soporte. Sin lugar a dudas es mucho más fácil administrar y dar soporte a varias máquinas desde un mismo equipo que hacerlo en cada uno de los equipos. El soporte y la administración centralizada de manera remota también son sumamente útiles en redes cuyas máquinas se encuentran en lugares muy distantes inclusive a nivel mundial.

El uso de las redes se refleja en la eficiencia y en un ahorro en recursos directos como impresoras y escáneres y en recursos indirectos como viáticos. En definitiva, el uso de las redes aumenta la eficiencia y reduce los costos de operación.

[1] El cable cruzado se muestra en la figura 1.27.

1.3 LANs y WANs

Las redes se dividen en dos categorías según su alcance geográfico, tamaño y función; en redes de área local: LANs (*Local Area Networks*) y redes de área global: WANs (*Wide Area Networks.*)

Una LAN está definida como una red confinada a un área geográfica limitada y puede ser desde un par de computadoras conectadas entre sí directamente por medio de un cable hasta cientos o aún miles de computadoras conectadas entre sí dentro de una gigantesca empresa.

La definición más prolífica de lo que es una WAN dice que una WAN consta de varias LAN interconectadas y que no tiene limitaciones geográficas.

Analícese el siguiente ejemplo: Juan y Rosa son adolescentes comunes y, como tales, están familiarizados con el mundo de las redes (principalmente para bajar música y para conversar en línea.) En una ocasión, ambos están en el mismo café Internet y sin saberlo comienzan a platicar por medio de una aplicación en Internet. ¿Qué están utilizando? ¿Una LAN o una WAN?

Lo primero que se nota al considerar este ejemplo es que las definiciones tradicionales de LAN y de WAN se están tornando obsoletas. Se puede decir que los muchachos están utilizando una LAN, ya que las computadoras están conectadas en red dentro de un área geográfica perfectamente limitada, en este caso el café Internet y esto es correcto. Sin embargo, también se puede decir que están utilizando una WAN, ya que el servicio que están empleando se encuentra en Internet y por lo tanto las señales entre las máquinas viajan por una ruta prácticamente indefinida y sin límites geográficos definidos.

Microsoft da una definición un poco más concreta para diferenciar una WAN de una LAN; Microsoft dice que una LAN es una red que se encuentra dentro de un diámetro definido de hasta 2.5 Km. Y una WAN la red que sobrepasa este tamaño de diámetro.

Para Cisco, y para propósitos de exámenes de Cisco esta definición es la que ellos quieren oír, una red tipo WAN es aquella en la que las señales entre los equipos que se comunican viajan a través de una infraestructura en la que interviene alguno o varios de los siguientes elementos pertenecientes a terceros, como un ISP (*Internet Service Provider*): ruteadores, líneas telefónicas o dedicadas (incluyendo las inalámbricas), o satélites. Consecuentemente una red tipo LAN es aquella en la que en la conexión que las máquinas utilizan para comunicarse no participan dichos elementos o, si lo hacen, éstos pertenecen al mismo organismo, empresa o persona a quien pertenecen las máquinas. ¡Una razón por la que la definición oficial de estos tipos de red no ha cambiado es obviamente la ambigüedad de las definiciones modernas!

Véase la figura 1.2. De acuerdo a la definición de Cisco, en este escenario en que una antena une la señal entre dos edificios, se tratará de una red tipo LAN si el mismo organismo es dueño de ambos edificios y de la infraestructura (antenas) que se encarga de la transmisión. De cualquier otra forma, se tratará de una WAN.

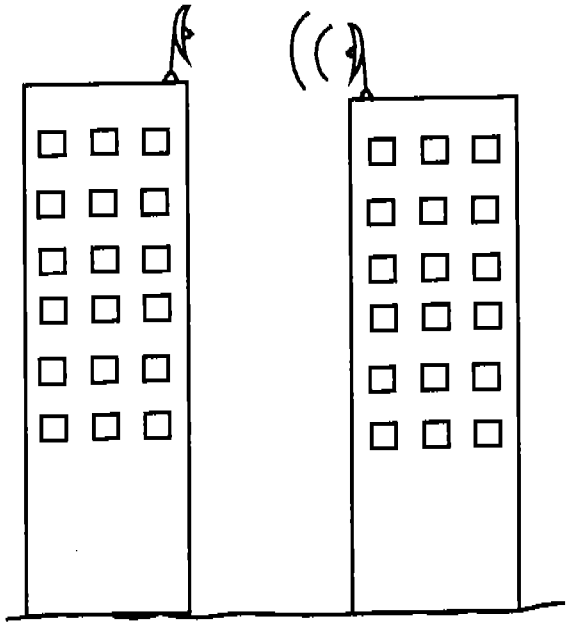


Figura 1.2 ¿WAN o LAN?

1.4 Redes Punto a Punto y Redes Cliente Servidor

Existen dos modelos básicos de redes, basándonos en los roles que las máquinas jueguen en ellas: las redes punto a punto y las redes cliente servidor.

Una red punto a punto es aquella en la que todas las máquinas tienen el mismo nivel jerárquico y no cuentan con una administración centralizada. El término en inglés *peer to peer*[2] describe mejor esta idea. En una red punto a punto cada usuario tiene libertad en cuanto a qué recursos comparte y cada usuario es responsable de la seguridad relacionada directamente con su máquina. Generalmente, cuando la seguridad está a cargo de todos, está a cargo de nadie. Cada máquina comparte información que almacena en su propio disco por lo que mientras más grande es la red punto a punto, es más difícil localizar y respaldar información esencial para varios usuarios.

Las redes punto a punto también son conocidas como grupos de trabajo y aunque las máquinas miembro de estos grupos de trabajo pueden tener sistemas operativos para cliente o para servidor, no hay ningún servidor dedicado a atender las necesidades de la red.

[2] *Peer* significa compañero

Las redes punto a punto son, generalmente, más baratas y fáciles de implementar que las redes bajo el modelo cliente-servidor y, no requieren de personal especializado para su implementación o mantenimiento. Sin embargo, en la práctica este modelo de redes funciona en ambientes pequeños en los que tan solo un número limitado de computadoras se interconectan y los recursos y archivos que se comparten son pocos.

Por regla general se recomienda que una red bajo el modelo punto a punto no tenga más de 10 computadoras.

El modelo cliente-servidor es el mayormente implementado hoy en día. Las ventajas de este modelo se derivan principalmente de la administración centralizada que se puede tener. Esta administración centralizada incluye manejo de cuentas de usuario, seguridad y procedimientos de respaldo.

En una red tipo cliente-servidor, el número de máquinas está limitado por la capacidad del servidor y puede llegar a ser de algunos miles. La seguridad de la red y de las máquinas en particular se administra de manera centralizada por lo que es mucho más robusta que en el modelo cliente-servidor. Sin embargo, se requiere de personal especializado para implementar, configurar, mantener y dar soporte a una red bajo este modelo.

Los costos de implementación son mayores al utilizar una red cliente-servidor y son normalmente más complejas que al instalar una red punto a punto.

1.5 Topologías de Red

El término topología se refiere a los esquemas físico y lógico en los que se basa una red. El esquema físico es la ubicación real de los dispositivos de conexión, cables y computadoras en el área de implementación de la red, mientras que el esquema lógico es la manera funcional en que los componentes están conectados entre sí. Entre las topologías más comúnmente utilizadas actualmente se encuentran la de bus, estrella, anillo, malla e inalámbrica.

1.5.1 Topología Bus

La topología bus utiliza un cable coaxial llamado bus o espina dorsal a la que se unen todas las computadoras en una sola línea a través de conectores "T". La información de la red en la forma de señales electrónicas digitales se manda sobre el bus a todas las computadoras de la red. Sin embargo, únicamente la computadora hacia la que va dirigida la información acepta la señal. Solo una computadora puede mandar información a la vez. En esta topología, todas las computadoras reciben y leen el encabezado de cada paquete y si su dirección no coincide con la dirección de destino en el encabezado, entonces el paquete se deriva a tierra sin mayor lectura. Este tipo de lectura llamada pasiva permite que cada computadora sea responsable

tan solo de recibir la información para ella misma y no de recibir y reenviar información destinada para otra computadora por lo que si una computadora llega a fallar, esto no afecta al resto de la LAN. Dadas las características del cable coaxial, en los extremos del mismo se forma un capacitor, el cual produce un efecto de rebote de la señal no deseado. Este rebote viaja de extremo a extremo sobre el cable cada vez volviéndose más débil pero provocando colisiones e impidiendo que cualquier transmisión sobre la red sea posible. Para eliminar dicho efecto, en cada extremo de un bus se pone un terminador que no es más que una simple resistencia de 50Ω. En el caso de que el cable tuviera una ruptura, se tendrían nuevos extremos en el cable, extremos sin un terminador, por lo que la señal nuevamente rebotaría chocando con la información enviada y por ende impidiendo cualquier comunicación por medio del bus. En la figura 1.3 se muestra un ejemplo de esta topología.

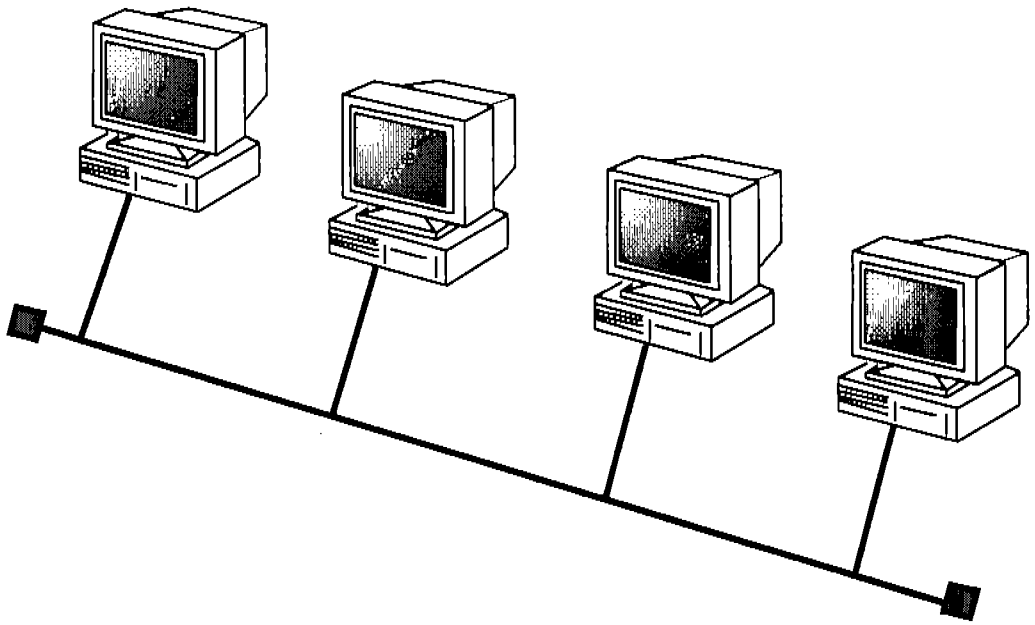


Figura 1.3 Topología bus

Método de acceso es la manera en que se organizan los dispositivos en una red para hacer uso del medio de transmisión. En otras palabras, el método de acceso es cómo las computadoras ponen las señales en el cable o medio de transmisión de manera que dichas señales no se interrumpan mutuamente.

El método de acceso que la topología bus utiliza se conoce como CSMA/CD (*Carrier Sense Multiple Access With Collision Detection*)[3]. En este método, la computadora que intenta transmitir datos "detecta" si hay datos en el medio y solo transmite si no los hay, mientras esta computadora está transmitiendo, obviamente hay datos en el medio por lo que ninguna otra computadora puede transmitir.

[3] Acceso múltiple por detección de portadora con detección de colisiones

Cuando los datos han llegado a su destino el medio vuelve a estar libre y las computadoras que necesitan transmitir contienden por ser la siguiente en tomar el medio (contienden en velocidad por transmitir antes que otra lo haga) es por eso que CSMA/CD es un método de contención. En algunas ocasiones, dos máquinas comienzan a transmitir exactamente en el mismo ciclo de reloj de sus procesadores, ya que ambas detectaron un ciclo antes que el medio estaba libre y podían transmitir. En estos casos, los datos que ambas máquinas ponen en el medio se alteran mutuamente, a esto se le conoce como una colisión. Al mandar información al medio, cada máquina guarda una copia del paquete enviado misma que compara con el paquete que se encuentra en el medio, si ambos paquetes no son iguales, entonces se sabe que una colisión ha ocurrido. Esta característica es la que aporta el modificador /CD (*collision detection*) al nombre del método. Cuando se detecta una colisión ambas computadoras entran a un periodo de espera semi-aleatorio basado en su posición en la red determinado por un algoritmo llamado *Backoff Algorithm.*

Mientras más equipos se tengan en la red habrá más tráfico y por lo tanto más colisiones y las máquinas que participaron en la colisión tendrán que retransmitir sus datos generando aún más tráfico y por consiguiente más colisiones con paquetes de otros equipos. Este proceso puede llegar a ralentizar la red e incluso paralizarla.

Las ventajas de esta topología con respecto a otras son:

- Es barata.
- Es fácil de instalar.
- Requiere menos cable que otras topologías.
- No requiere de un equipo especializado.

Las desventajas de esta topología son:

- Puede haber disrupción en la red al quitar o añadir dispositivos.
- Como todos los sistemas en la red accesan a una misma espina dorsal, una ruptura en el cable evitará que cualquier sistema pueda trabajar en red.
- Es una de las topologías más difíciles de arreglar cuando falla.

1.5.2 Topología Estrella

La topología estrella es, sin duda, la más utilizada actualmente y hay razones para ello.

En esta topología, todas las computadoras y demás dispositivos se conectan a un concentrador que puede ser un *hub* o un *switch*[4]. Cada dispositivo se conecta al

[4] Estos dispositivos se ven a mayor detalle en la página 35.

concentrador con un cable independiente creando una conexión punto a punto[5] entre el dispositivo y el concentrador.

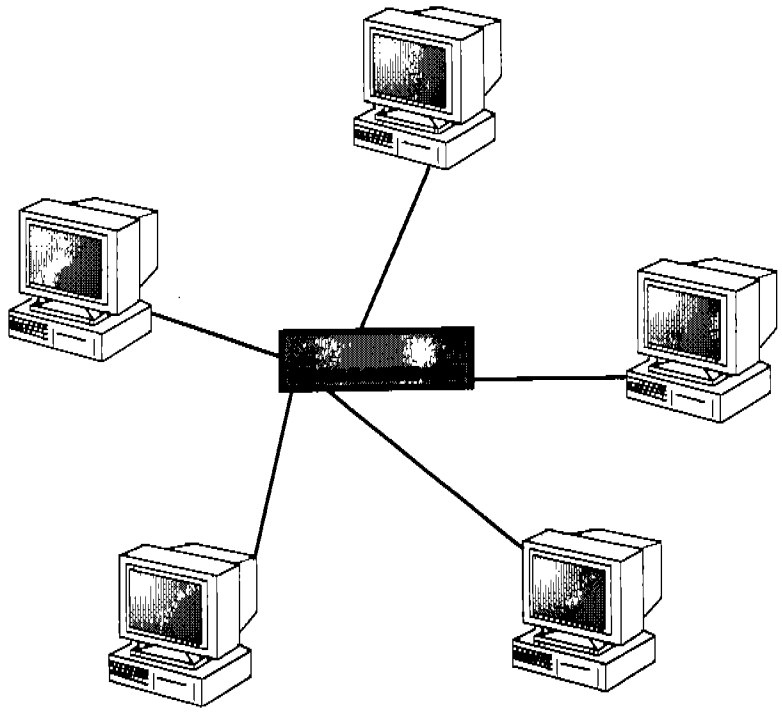


Figura 1.4 Topología estrella

Al estar conectadas por diferentes cables, cada computadora con el concentrador, no es necesario que la red deje de funcionar para añadir o quitar computadoras y si alguna computadora falla o algún cable llega a fragmentarse, esto afecta solamente a la computadora que tiene el problema. Por esto, la topología estrella es la más fácil de expandir. La figura 1.4 muestra un ejemplo de la topología estrella..

Dado el concentrador y el número de cables que se requieren para esta topología, una estrella es más cara de implementar que un bus.

Esta topología también utiliza como método de acceso CSMA/CD con la diferencia que ahora el medio de transmisión que las máquinas están monitoreando (para ver si está libre y pueden transmitir), incluye un concentrador.

Las ventajas de la topología estrella son:

- Fácil de expandir sin interrumpir a los usuarios de la red.
- La ruptura de un cable afecta solamente a una computadora.
- Los problemas son fáciles de aislar.

[5] Una conexión punto a punto es aquella en que dos dispositivos se conectan directamente y de manera exclusiva por un cable u otro medio. Téngase cuidado de no confundir una conexión punto a punto con una red punto a punto.

- Es relativamente fácil de arreglar cuando falla

Las principales desventajas de una estrella son:

- Requiere más cable que otras topologías.
- Si el concentrador llega a fallar, ninguna máquina podrá accesar a la red.
- Es más difícil de implementar que otras topologías.

1.5.3 Topología Anillo

La topología anillo (o *token ring*) es, de hecho un anillo lógico ya que los datos viajan de una computadora a otra de manera circular. (Un dato curioso es que IBM define que los datos viajan de manera circular en dirección contraria a las manecillas del reloj mientras la IEEE dice que lo hacen en dirección de las manecillas del reloj. ¡Algo que carece de significado en el mundo real!.)

Este anillo lógico se puede implementar de manera física como un anillo físico o como una estrella. Véanse las figuras 1.5 y 1.6.

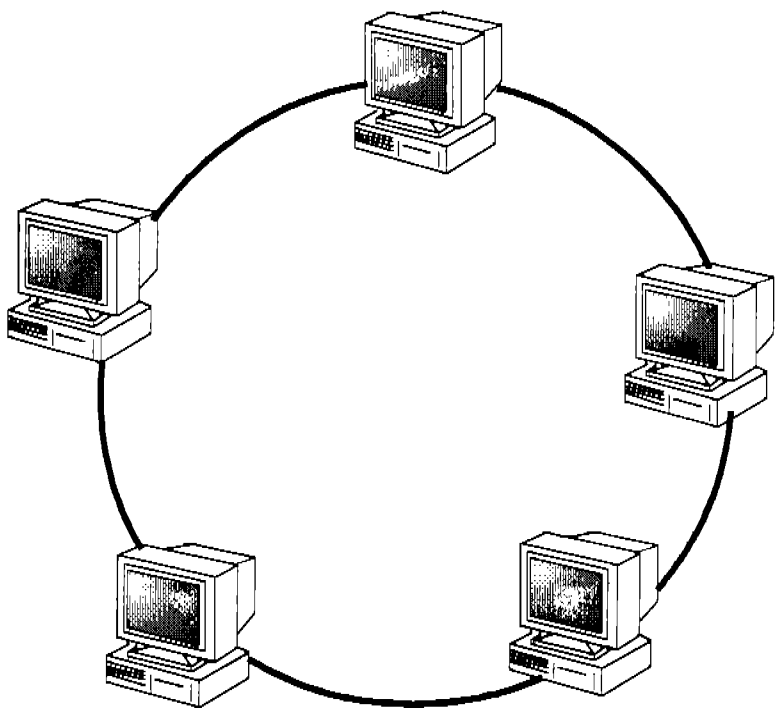


Figura 1.5 Topología lógica de anillo y topología física de anillo.

En la topología de anillo lógico implementada con un anillo físico, si una computadora falla o un cable se troza toda la red dejará de funcionar. También si se necesita agregar o quitar una computadora a la red, es necesario que la red completa deje de funcionar. Por esta razón, una red en anillo físico no es una buena opción para entornos con cambios constantes.

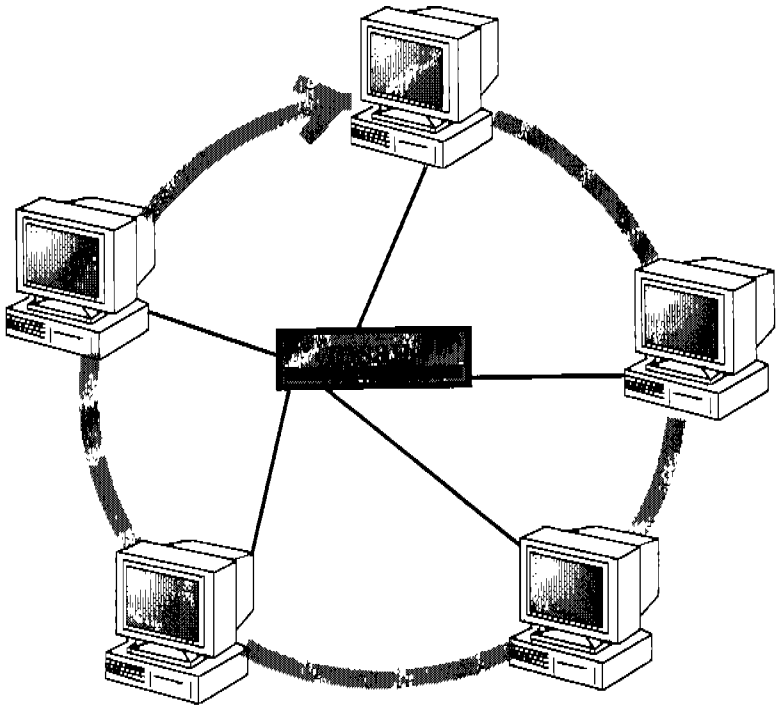


Figura 1.6 Topología lógica de anillo y topología física de estrella.

Las redes en anillo muy frecuentemente se implementan de manera física como estrellas con la diferencia de que el concentrador en este caso no es un *hub* o un *switch* sino un MSAU (*Multistation Access Unit.*) El MSAU dirige internamente el flujo de la información de manera que ésta siga el curso de un anillo lógico.

El método de transmisión que utiliza el anillo es *Token Passing* o pase de estafeta. En este método, la primera computadora que se prende genera un paquete vacío llamado *token* o estafeta. El *token* generado comienza a circular en la red en el orden diseñado (por supuesto que físicamente no tiene que ser en círculo.) Cada máquina recibe y lee la totalidad del *token* y entonces lo manda a la siguiente máquina en la ruta alrededor del anillo. Solamente puede haber un *token* a la vez en el anillo y para transmitir, las máquinas deben esperar a recibir un *token* vacío en donde pondrán la información y un encabezado que contiene, entre otros datos, un identificador de la máquina origen y un identificador de la máquina destino. La máquina que llenó el *token* lo deposita en la red, en donde cada máquina leerá toda la información (no sólo el encabezado como pasa en CSMA) y lo regresará a la red hasta que el *token* arribe a la máquina destino la cual, al igual que el resto de las computadoras leerá toda la información y lo depositará completo en la red (con la diferencia de que pasará la información a su sistema operativo además de añadir una bandera al paquete que indica que el mensaje se recibió correctamente), se podría pensar que a partir de este momento las máquinas siguientes no perderán tiempo en leer todo el *token* y redepositarlo en la red, sin embargo, no es así. Las máquinas que reciben el *token* después de que éste llegó a su destino lo reciben completo, lo leen completo y

lo depositan completo de nuevo en la red. Esto sucede hasta que la máquina que depositó la información en el *token*, la máquina origen, recibe el *token* e identifica que el paquete llegó con bien a su destino. Entonces la máquina origen destruye el *token* y genera uno nuevo, que pone a circular en la red.

El método de *token passing* no parece ser muy eficiente, pero tiene puntos muy fuertes a favor: en primer lugar el *token* puede viajar a velocidades cercanas a la de la luz, además, por haber un solo *token* en la red en cualquier momento dado, es imposible que se produzca una colisión. Aún el hecho de que cada máquina recoja todo el *token* y luego lo regrese a la red sirve a un propósito: al viajar por un medio impuro y sujeto a estímulos externos, la señal en el cable se altera y se debilita pero cada máquina funciona como un amplificador y regenerador de la señal, permitiendo distancias mayores entre las máquinas.

La primera máquina que se prende, se constituye como el monitor de la red y se encarga de revisar la integridad de los paquetes que viajan sobre ella y que en ningún momento haya más de un *token* en la red, además, cada 7 segundos envía sobre la red un paquete muy ligero que se llama *beacon* o indicador. El *beacon* pasa de máquina en máquina por todo el anillo, si un equipo no recibe el *beacon* enviará al monitor de la red un mensaje de aviso de que la conexión se ha perdido. En este mensaje se incluye su dirección y la dirección de la máquina que no transmitió el *beacon*. A partir de esta información, el monitor intenta diagnosticar el problema y a prueba y error manda comandos de control a la máquina que no transmite el *beacon* para tratar de solucionar el problema, tratando que la red no se caiga definitivamente.

Ventajas de la topología anillo:

- Los cables estropeados son fáciles de localizar.
- Los problemas con la red son relativamente fáciles de resolver.
- La falla de una computadora no interrumpe la comunicación en red de las otras computadoras. (en anillo lógico y estrella física)
- Cada máquina actúa como un repetidor (amplifica y regenera la señal.)
- La topología anillo es relativamente fácil de implementar

Desventajas de la topología anillo:

- No se pueden añadir máquinas sin deshabilitar toda la red.
- En el caso del anillo físico, un solo cable dañado puede hacer que toda la red deje de funcionar.
- En el caso de anillo lógico y estrella física, toda la red deja de funcionar si el concentrador (MSAU) falla.

1.5.4 Topología Malla.

La topología malla o mesh basa su implementación en la necesidad que algunos ambientes específicos tienen de confiabilidad de transmisión a nivel físico. La malla hace posible que una red funcione normalmente, aún con múltiples cables trozados o defectuosos. Para lograr esto se utiliza una solución de "fuerza bruta", que consiste en conectar todos los dispositivos en la red con cada uno de los demás. Véase la figura 1.7. La malla es sumamente escasa en ambientes LAN.

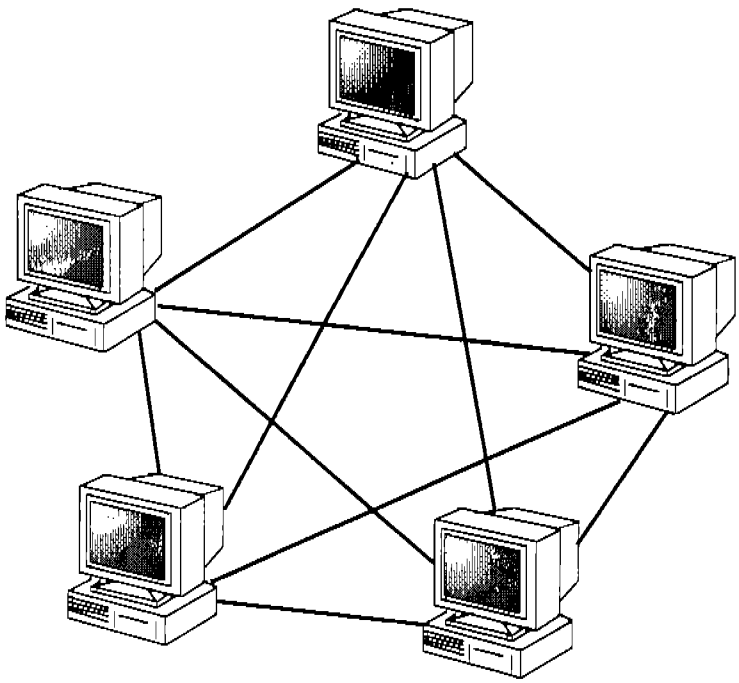


Figura 1.7 Topología Malla

La implementación de esta topología puede ser muy complicada y el costo de cableado es obviamente mucho mayor que en otras topologías. Además, dado el nivel de redundancia, muchas veces es difícil notar que algún cable está fallando y cuál es.

En una malla de n máquinas, se tienen un total de $(n^2-n)/2$ cables de interconexión, de los cuales pueden fallar hasta $(n^2-3n+2)/2$ sin que una sola de las máquinas en dicha red quede incomunicada.

Una variante de la topología mesh pura en la que cada uno de los dispositivos se conecta a todos los demás, es la mesh híbrida en la que solo algunos dispositivos específicos se conectan con rutas redundantes, este tipo de topología se encuentra fácilmente en Internet y ambientes WAN.

Ventajas de la topología malla:

- Provee rutas redundantes entre los dispositivos de la red por lo que hay gran tolerancia a fallos de cableado.
- La red puede expandirse sin interrupción a los usuarios.

Las desventajas más importantes de la topología malla son:

- Requiere más cable que otras topologías.
- Encontrar un cable que esté fallando puede ser muy difícil.
- Como la red sigue funcionando aún con varios cables segmentados, es posible no notar errores en los cables sino hasta que son demasiados los cables con errores.

1.5.5 Topología Inalámbrica

En la topología inalámbrica, tal como el nombre lo sugiere, no se requieren cables para la interconexión de las computadoras. El principal beneficio de esta topología es obvio, tener acceso a los recursos de la red sin necesidad de cableado. Véase la figura 1.8.

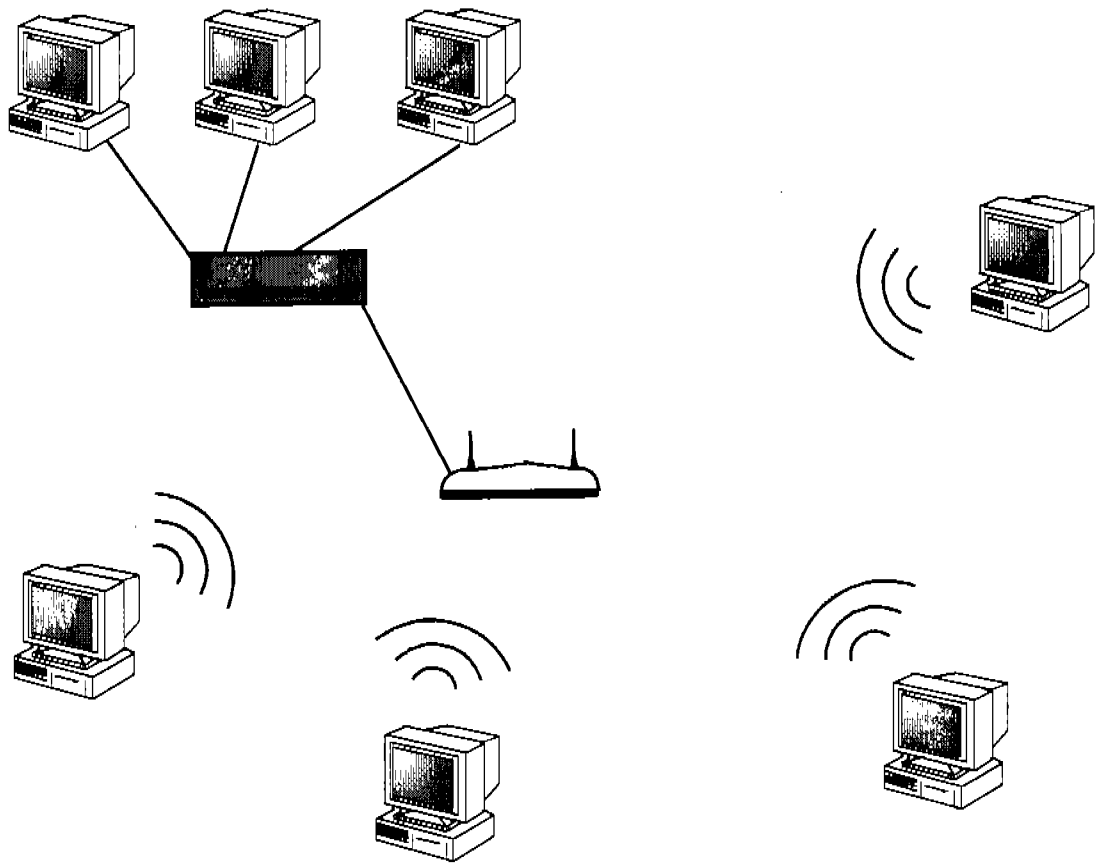


Figura 1.8 Ejemplo del uso de una topología inalámbrica.

La topología inalámbrica elimina los problemas relacionados con rupturas o fallas de cables pero introduce sus propios problemas. En específico incluye dos problemas principales: el primero, dado que el medio de transmisión (el aire) es abierto, la seguridad en una red inalámbrica muchas veces se ve comprometida y, el segundo, las señales son muy susceptibles a tener interferencia. Aunque muchos problemas de seguridad ya se han resuelto satisfactoriamente, la reputación de la seguridad de la red inalámbrica sigue siendo mala.

Para la implementación de esta red se utiliza un dispositivo llamado "Punto de Acceso Inalámbrico" o WAP para que los dispositivos inalámbricos se conecten en red. La topología inalámbrica es particularmente útil en ambientes con varios usuarios con laptops.

El método de acceso que la topología inalámbrica utiliza es CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance.*) Este método es igual a CSMA/CD con la diferencia que cuando alguna máquina tiene información por transmitir, antes de transmitirla envía un pequeño paquete con el cual avisa a las demás máquinas de la red su intención de transmitir. De esta manera se evita la posibilidad de que se produzcan colisiones y se pierda información sobre la red. La desventaja de este método es que el envío de los paquetes de intención, provoca por sí mismo considerable tráfico haciendo, por lo tanto, más lenta la red.

Las ventajas de utilizar una topología inalámbrica son:

- La comodidad de los usuarios, gracias al acceso remoto inalámbrico.
- La red se puede expandir sin interrupción a los usuarios.

Algunas desventajas son:

- La velocidad de transmisión es todavía muy limitada con respecto a lo logrado con otras topologías.
- La seguridad en una red inalámbrica puede no ser la óptima.

1.6 Estándares de la IEEE para Redes

El Instituto de Ingenieros Electrónicos y Electricistas (IEEE) desarrolló una serie de estándares para las redes para asegurar que las tecnologías de diversos fabricantes sean compatibles. En otras palabras, si los fabricantes en el campo de las redes cumplen con los estándares de la IEEE, entonces los cables, dispositivos de red, protocolos, etc. serán intercambiables sin importar el fabricante de los mismos. Los estándares para la industria de las redes fijados por la IEEE son los estándares 802. La tabla 1.1 muestra los estándares 802.

Especificación	Nombre
802.1	Interconexión de redes
802.2	LLC (logical Link Control)
802.3	CSMA/CD para Ethernet
802.4	Token passing
802.5	Redes Token ring
802.6	Man (Metropolitan Area Network)
802.7	Banda Ancha
802.8	Fibra Óptica
802.9	Redes con Voz y Datos integrados
802.10	Seguridad
802.11	Redes inalámbricas
802.12	100 VGAny LAN

Tabla 1.1 Estándares 802 del IEEE.

El examen solo cubre algunos de los estándares 802 del IEEE: 802.2, 802.3, 802.5 y 802.11.

1.6.1 Estándar 802.2 del IEEE

El estándar 802.2 del IEEE conocido como LLC (*Logical Link Control*), se encarga de manejar el flujo de datos y el control de errores en la transmisión entre dispositivos.

El control de flujo regula la cantidad de datos que se pueden transmitir en cierto intervalo de tiempo. Mientras que, el control de errores se refiere a la identificación y notificación de señales dañadas. Esto último se logra a través de un algoritmo de conteo que genera un número a partir de los datos en un paquete al momento de transmitirse, este número se incluye en el mismo paquete. Al arribar el paquete a su destino, se genera nuevamente el número con el mismo algoritmo y se coteja con el número que se anexó en el otro extremo. Si estos números son diferentes, entonces se ha identificado un error en la transmisión del paquete y, dependiendo del método de transmisión, se solicitará o no una retransmisión.

1.6.2 Estándar 802.3 del IEEE

El estándar 802.3 del IEEE define las características que las redes *Ethernet* deben tener. *Ethernet* es, por mucho, la más popular de las tecnologías utilizadas en las redes tipo LAN.

Se han hecho varias adiciones al estándar 802.3 original. Algunas de estas adiciones son el estándar 802.3u para tecnologías *Fast Ethernet* y el 802.3z para el *Gigabit Ethernet.*

La velocidad de transmisión del estándar original 802.3 era de 10Mbps. Sin embargo, el estándar 802.3u añadido después especifica una velocidad de transmisión de 100Mbps y el estándar 802.3z especifica una velocidad de hasta 1000Mbps.

Las primeras redes *Ethernet* utilizaban una topología bus o estrella porque el estándar original incluía especificaciones para ambos, cable coaxial y par trenzado. Los estándares 802.3u y 802.3z especifican par trenzado y topología estrella, y algunos estándares más modernos especifican fibra óptica como medio de conexión. Aún utilizando una topología física estrella, *Ethernet* utiliza una topología lógica bus.

El método de acceso definido por el estándar 802.3 para *Ethernet* es *Carrier Sense Multiple Access with Collision Detection* CSMA/CD.

1.6.3 Estándar 802.5 del IEEE

El estándar 802.5 del IEEE especifica las características que regulan a las redes anillo (*token ring.*) *Token ring* tuvo gran auge, impulsada por IBM, a mediados de los 80's, lo que la convirtió en la topología más popular por algún tiempo, tiempo que fue marcado por el avance de *Ethernet.* Hoy en día es difícil encontrar un *token ring* y mucho más difícil tener que implementar uno en una nueva red.

Las características definidas en el estándar 802.5 definen la velocidad de las redes *token ring* a 4Mbps y a 16Mbps y su topología como una topología de anillo lógica aunque muy frecuentemente se implementa a través de una estrella física con un dispositivo coordinador llamado MSAU.

Las redes *token ring* utilizan par trenzado como su medio de conexión y *token passing* como su método de acceso.

1.6.4 Estándar 802.11

El estándar 802.11 especifica las características que debe tener una red inalámbrica. Este estándar se puede implementar de varias formas, pero la más común es por medio de radio frecuencia utilizando dispositivos conocidos como WAP's (*Wireless Access Points.*)

Dentro del estándar 802.11 existen varios estándares adicionados conforme el aumento en la tecnología, los más importantes son el 802.11b, el 802.11g y el 802.11a.

El estándar 802.11b especifica velocidades de transmisión de 11Mbps sobre radio ondas de 2.4Mhz. El estándar 802.11g especifica velocidades de transmisión de 22Mbps (actualmente alcanzan hasta 54Mbps) sobre radio ondas de 2.4Mhz.

El estándar 802.11a especifica velocidades de transmisión de 50 a 54Mbps sobre radio ondas de 5Mhz.

El método de acceso que el estándar 802.11 utiliza es CSMA/CA, el cual es una variación en la que se evitan las colisiones, de CSMA/CD. El estándar 802.11 utiliza una topología física inalámbrica y como su tecnología está basada en *Ethernet* funciona con una topología lógica bus.

Las redes inalámbricas pueden utilizar varios diferentes medios de transmisión como radio frecuencias en diversos rangos y microondas. Y sus alcances varían de acuerdo al medio de transmisión empleado desde algunos metros hasta algunos cientos de metros.

1.6.5 FDDI

Otro estándar importante es uno desarrollado por la ANSI (*American National Standards Institute*) a mediados de los 80's y es el FDDI (*Fiber Distributed Data Interface.*)

El FDDI utiliza una topología similar a la del anillo tradicional, pero con la diferencia de que el anillo es doble y el *token* en cada anillo viaja en dirección opuesta a la que lleva el otro *token*. Véase la figura 1.9.

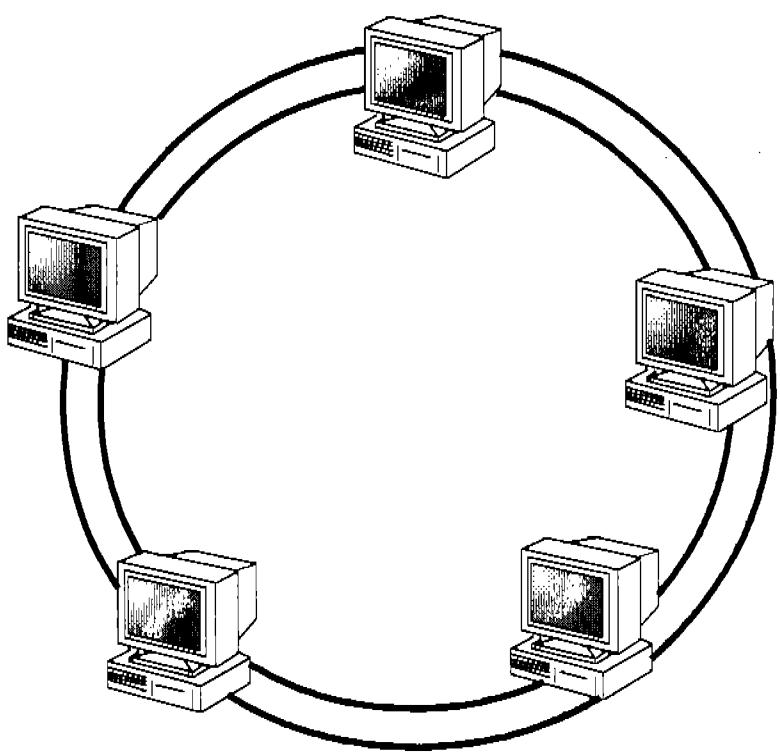


Figura 1.9 Red FDDI

El segundo anillo se implementa para proveer redundancia y consecuentemente tolerancia a fallos de transmisión en la red. Por este motivo, generalmente no se utiliza el segundo anillo en la red a menos que falle el primero. Sin embargo, es posible configurar el anillo para que algunos usuarios privilegiados utilicen el segundo anillo cuando el *token* en el primer anillo no esté disponible.

La velocidad a la que transmite un FDDI es de 100Mbps o mayor sobre un medio de fibra óptica que permite distancias de transmisión que exceden los dos kilómetros

El método de acceso de FDDI es, como en el caso de *token ring*, *token passing*.

Es posible aplicar los estándares de FDDI sobre cables de cobre. A esta implementación se le conoce como CDDI; Copper Distributed Data Interface.

1.7 Consideraciones para Medios de Transmisión.

Al trabajar con alguna red existente o al implementar una red, es importante que se tenga conocimiento de las características de diferentes medios de transmisión, incluyendo el cableado de interconexión y sus conectores asociados. Sin embargo hay consideraciones generales que se deben hacer para elegir el mejor medio de transmisión para cada diferente escenario.

1.7.1 Banda ancha y base banda

Las redes emplean dos métodos para la transmisión de señales: banda ancha y base banda. Las transmisiones en base banda utilizan señales digitales sobre un solo cable. Las transmisiones base banda pueden ser bidireccionales, es decir, se puede transmitir y recibir por el mismo cable aunque no al mismo tiempo. El método de transmisión por base banda puede permitir enviar y recibir múltiples señales por el mismo cable a través de la multiplexión por división en tiempo o TDM.

Otra manera de ver el TDM es que las señales toman turnos para utilizar el cable y que estos turnos tienen una duración predeterminada muy pequeña por lo que el paquete original que se desea transmitir se divide en varios paquetes más pequeños (que se pueden enviar en el intervalo predeterminado), a los usuarios de la red esto les parece que ocurre "al mismo tiempo" por que los turnos tienen duraciones imperceptiblemente pequeñas para los sentidos del hombre.

Las transmisiones que se hacen por el método de banda ancha utilizan señales analógicas moduladas por frecuencia. Para poder transmitir múltiples señales sobre el mismo cable, se utiliza la multiplexión por división de frecuencias o FDM. La FDM divide la frecuencia total que el cable soporta en varios canales que se pueden utilizar simultáneamente por diferentes señales y en cualquier dirección.

1.7.2 *Simplex, half duplex* y *full duplex*

Cualquier sistema de comunicaciones puede ser catalogado como *simplex*, *half duplex* o *full duplex*.

En los sistemas *simplex*, el medio de transmisión maneja el flujo de información en un solo sentido. Un ejemplo de este tipo de transmisión es el envío de un telegrama. Al enviar un telegrama, el emisor entrega la información que desea transmitir y esta información alcanza al receptor. Sin embargo, el receptor no puede responder con ese telegrama por lo que el emisor no tiene retroalimentación o confirmación de que la información se ha recibido satisfactoriamente.

En un sistema de transmisión tipo *half duplex*, el medio de transmisión se utiliza en ambos sentidos pero no simultáneamente. Siguiendo la línea de las comunicaciones cotidianas, un ejemplo de este tipo de sistemas es el walkie talkie. Para comunicarse por walkie talkie la persona que quiere hablar mantiene presionado un botón de "hablar" mientras lo hace y la otra persona solamente escucha mientras la primera habla. Cuando la persona que hablaba termina de hacerlo, suelta el botón y entonces su aparato se convierte en receptor para que el interlocutor presione el botón de "hablar" y responda. Si ambas personas presionan el interruptor de hablar, ambos aparatos envían pero ninguno recibe señal alguna. O si ambas personas solamente esperan recibir sin que ninguna transmita el canal permanecerá vacío y no habrá comunicación.

El último tipo de diálogo que existe es el *full duplex*. En este sistema, ambas partes de la comunicación pueden transmitir y recibir en cualquier momento, incluso simultáneamente. Volviendo a la analogía con las comunicaciones cotidianas; un sistema *full duplex* es el teléfono.

1.7.3 Interferencia

A las señales o ruidos externos que de algún modo se suman a la señal transmitida por un canal y que afectan los datos de manera no deseada se les llama interferencia. Existen dos tipos de interferencia que pueden afectar una transferencia en red: interferencia electromagnética (EMI) y señales cruzadas (*crosstalk.*)

Cualquier flujo de electrones produce un campo magnético alrededor del medio que lo contiene. Este campo magnético se mueve según la regla de la mano derecha; al tomar con la mano derecha el cable por el cual los electrones fluyen y apuntar con el dedo gordo en la dirección hacia la que fluyen los electrones, los demás dedos se doblan en el sentido en el que se mueve el campo magnético generado.

En el caso de la EMI, el campo magnético es generado por dispositivos eléctricos tales como una bomba de agua, aire acondicionado o balastros de luz fluorescente. Si el cable de red pasa lo suficientemente cerca de estos dispositivos, la señal en el cable puede corromperse ya que el campo magnético es suficientemente fuerte como

para provocar alteraciones en los electrones que viajan sobre el cable. Diferentes cables tienen diferentes tolerancias a la EMI.

En la interferencia crosstalk, dos señales viajando por medios separados se interfieren mutuamente provocando que ambas señales resulten corruptas. Así como en el caso de EMI existen diferentes tolerancias al crosstalk para diferentes medios, por ejemplo, tanto el EMI como el crosstalk son nulos para el caso de la fibra óptica mientras que hay que considerarlos cuidadosamente en la planeación de redes con cables UTP.

1.7.4 Atenuación

Un efecto que se debe considerar al hablar de medios de conexión es la atenuación. La atenuación se produce al transmitir cualquier señal por cualquier medio ya que actualmente cualquier medio de transmisión absorbe energía. En el caso de transmisiones por cable de cobre, las señales viajan gracias al efecto dominó de los electrones sobre el medio pero cada átomo de cobre absorbe una pequeña cantidad de energía que en distancias grandes se vuelve considerable, esto aunado a las impurezas del cable resultan en la atenuación de la señal. En el caso de la fibra óptica, la señal viaja en forma de luz por lo que pequeños cuerpos opacos en el cable debilitan la señal conforme esta viaja sobre la fibra óptica. La atenuación va relacionada con la distancia máxima de transmisión sobre un medio, si esta distancia se excede se pueden presentar problemas de red muy difíciles de resolver.

1.7.5 Ancho de banda

Una de las consideraciones más importantes que hacer respecto a medios de transmisión es el ancho de banda. El ancho de banda es la capacidad de transmisión de datos que un medio tiene y se mide en *bit*s por segundo (bps.) En otras palabras, el ancho de banda es la cantidad de *bit*s que un medio puede acarrear en un segundo. Los medios de transmisión hoy en día pueden soportar anchos de banda en el orden de los Mbps y hasta Gbps. La gran mayoría de las redes de aplicaciones requieren más que los 10Mbps que ofrecían las primeras redes *Ethernet*, en algunos casos aún los 100Mbps que ofrecen muchas de las LANs modernas no son suficientes para satisfacer los requerimientos de la red.

1.8 Medios de Transmisión

Existen dos tipos de medios de transmisión: los basados en cable y los asociados con transmisiones inalámbricas. Los basados en cable son: coaxial, fibra óptica y par trenzado; y los inalámbricos son radio ondas, rayos infrarrojos y microondas.

1.8.1 Cable coaxial

El cable coaxial es uno de los medios de transmisión más conocidos y utilizados. Este tipo de cable ha tenido gran éxito tanto en el ámbito de las redes como en transmisiones de televisión.

El cable coaxial se conforma como su nombre lo indica de cilindros de diferentes materiales que comparten el mismo eje; el centro del cable está hecho de cobre, el cual transporta la señal, rodeando al cobre hay una capa de aislante plástico, enseguida hay una malla metálica y por último una cubierta plástica. El diseño del cable coaxial lo hace muy resistente a interferencias electromagnéticas y crosstalk ya que el centro que acarrea la señal se protege por el efecto de la jaula de Faraday con la malla metálica que va conectada a tierra.

Actualmente el cable coaxial está cayendo en desuso dado el reducido ancho de banda que maneja. Sin embargo todavía es posible encontrar muchas redes implementadas con este tipo de cable. Hay dos tipos de cable coaxial que se usan en redes: cable coaxial delgado y cable coaxial grueso.

El cable coaxial delgado es más frecuentemente usado que el grueso, pero tampoco es muy común. El cable coaxial delgado es fácil de manejar porque tiene un diámetro de tan solo ¼". Desafortunadamente, esta misma característica determina una de las desventajas de utilizar coaxial delgado: Lo hace demasiado frágil y fácil de romper.

Existen diferentes tipos de cable coaxial delgado y cada uno tiene aplicaciones asociadas. La tabla 1.2 muestra las categorías de cable coaxial delgado.

Cable	Tipo
RG-58/U	Centro de cobre liso
RG-58 A/U	Centro de cable
RG-58 C/U	Especificación militar
RG-59	Utilizado para televisión por cable y cable módems
RG-62	Utilizado para especificaciones de redes ARCnet[6]

Tabla 1.2 Categorías de cable coaxial delgado

Cada vez, es más difícil encontrar dispositivos compatibles con este tipo de cable; tarjetas de red, *bridges* o *switches* que cuenten con conectores BNC se podrían considerar (humorísticamente) material especializado, por estar descontinuados y ser sumamente escasos.

[6] ARCnet es un estándar de redes obsoleto. Es importante tener cuidado de no confundir el cable RG-58 con el RG-62 ya que su apariencia es muy similar.

El cable coaxial grueso es sumamente difícil de encontrar hoy en día. Su categoría es RG-8 y es más robusto y difícil de dañar que la versión delgada. La construcción del cable coaxial grueso lo hace muy resistente a la atenuación, crosstalk y EMI por lo que es capaz de transmitir datos sobre grandes distancias. Gracias a esto, el cable coaxial grueso tuvo auge como *backbone* o espina dorsal de las redes. El cable coaxial grueso es más difícil de instalar y conectar que el cable coaxial delgado. Para conectar el cable coaxial grueso se utilizan conectores tipo vampiro. Los conectores vampiro son conectores en forma de caña que se acoplan al ancho del cable coaxial y tienen pequeños "colmillos" que perforan las protecciones del cable haciendo contacto con el centro y de esa manera derivando la información hacia la LAN.

1.8.2 Cable par trenzado

El cable par trenzado nació como una solución a los problemas de crosstalk en telefonía. Hoy es el medio más utilizado no solo en telefonía sino también en redes. La gran popularidad de que goza este medio se debe tal vez a que es ligero, flexible y más fácil de manejar e instalar que el coaxial o la fibra óptica. Además de tener un ancho de banda mucho mayor que su contraparte coaxial y un costo muchísimo menor que el de la fibra óptica.

El cable par trenzado se compone de uno o varios pares de cables de cobre con cubiertas individuales de plástico y con una cubierta también plástica para todos los pares. La razón del trenzado es anular los campos magnéticos que cada hilo genera. Al trenzar un cable con flujo de electrones en una dirección con otro con flujo en la dirección opuesta la mayor parte de los campos generados se anulan mutuamente. Esto resulta en una resistencia aceptable a crosstalk.

Existen dos tipos de par trenzado para redes: UTP (*unshielded twisted pair*) y STP (*shielded twisted pair.*) UTP es el más comúnmente usado pero en ambientes donde se requiere de una mayor protección contra EMI y atenuación es preferible el cable STP, ya que éste tiene, además de las características ya mencionadas, una cubierta de material metalizado antes de la cubierta de plástico exterior. Esta cubierta metalizada se aterriza para derivar a tierra las interferencias. Sin embargo, esta protección extra también tiene un costo extra además de necesitar conectores especiales para aterrizaje del cable. Véase la figura 1.10

Hay varias categorías de cables de par trenzado, las primeras se asocian más comúnmente con transmisiones de voz. Existen 7 categorías principales especificadas por la EIA/TIA (*Electronics Industries Association / Telecommunications Industries Association.*)

La tabla 1.3 muestra las 7 categorías de la EIA/TIA para cable par trenzado.

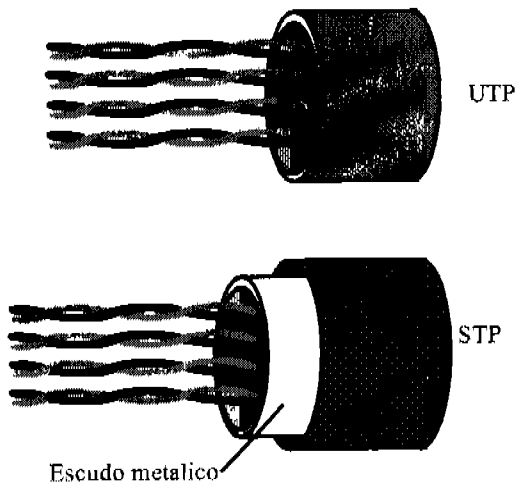


Figura 1.10 cables UTP Y STP

Categoría	Cable	Aplicación
1	UTP	Voz analógica
2	UTP	Voz digital, datos de 1Mbps
3	UTP, STP	Datos 16Mbps
4	UTP, STP	Datos 20Mbps
5	UTP, STP	Datos 100Mbps
5e	UTP, STP	Datos 155Mbps
6	UTP, STP	Datos 155Mbps
7	UTP, STP	Datos 1000Mbps

Tabla 1.3 Categorías de cable par trenzado

1.8.3 Cable de fibra óptica

El cable de fibra óptica resuelve muchos de los problemas asociados con los cables de cobre. Dado que la fibra óptica transmite luz en lugar de pulsos eléctricos, problemas tales como EMI o crosstalk simplemente no existen.

La fibra óptica es técnicamente un magnifico transmisor para video, datos y voz, además de que es capaz de un ancho de banda muy superior a otros medios. Dada la composición de la fibra óptica, ésta es sumamente segura para la transmisión de datos de carácter confidencial ya que para derivar una señal desde un cable de fibra óptica es necesario cortar el cable y derivar la luz, esto es muy difícil de hacer con las condiciones adecuadas y prácticamente imposible de hacer de manera furtiva.

La fibra óptica no es el más popular entre los medios de interconexión de redes por un sencillo detalle: el costo. La implementación de redes con fibra óptica es mucho más laboriosa y en algunos casos casi artesanal y por ende normalmente requiere de personal experto con equipo especializado. Otro de los problemas que trae consigo una solución con fibra óptica y que se refleja incrementando el costo, es que la mayoría de dispositivos de red no son compatibles con la fibra óptica. Por esta razón, al actualizar una red de cable de cobre a fibra óptica, realmente es necesario implementarla como si fuera nueva, ya que los dispositivos que se tienen no son compatibles con el nuevo cable.

Los cables de fibra óptica son filamentos de vidrio flexibles, a veces menores al espesor de un cabello humano, que llevan información en forma de haces de luz. El sistema de comunicación nace de una fuente de luz lo suficientemente pura para no alterarse. El cable de fibra está compuesto por dos capas de vidrio: la parte interior o núcleo es la que tiene mayor índice de refracción, es decir, por donde más fácilmente viaja la luz. La mayoría de las fibras ópticas se hacen de arena o sílice, materia prima abundante en comparación con el cobre.

Dos elementos esenciales de la fibra óptica son el núcleo y el revestimiento. El núcleo es la parte más interna de la fibra y es la que guía la luz. Consiste en una o varias hebras delgadas de vidrio o de plástico con diámetro de 50 a 125 micras. El revestimiento es la parte que rodea y protege al núcleo. El conjunto de núcleo y revestimiento está a su vez rodeado por un forro o funda de plástico que lo resguardan contra la humedad, el calor y otros riesgos del entorno. Véase la figura 1.11

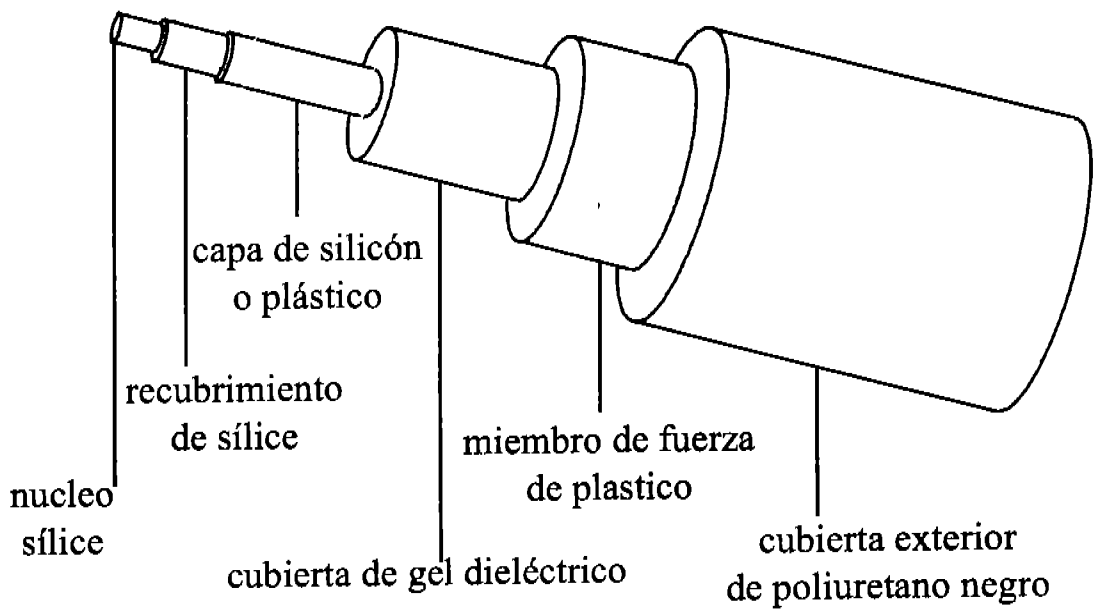


Figura 1.11 Cable de fibra óptica

Hay dos tipos de fibra óptica disponibles en el mercado: la fibra monomodo y la fibra multimodo. En la fibra monomodo un solo haz de luz viaja de extremo a extremo de manera directa por lo que el ángulo de incidencia debe ser desde -15° hasta 15° con respecto a la dirección del cable. En el cable multimodo, múltiples señales viajan por el mismo núcleo reflejándose por las paredes internas del cable. Por esta razón, en una longitud dada, la luz recorre mayor distancia en un cable multimodo que en uno monomodo. Y por supuesto, el cable monomodo es capaz de transmitir señales a distancias mayores que las que logra un cable multimodo.

Algunos de los tipos más comunes de cable de fibra óptico son:

- Núcleo de 62.5 micras – recubrimiento de 125 micras- multimodo
- Núcleo de 50 micras – recubrimiento de 125 micras- multimodo
- Núcleo de 100 micras – recubrimiento de 140 micras- multimodo
- Núcleo de 83 micras – recubrimiento de 125 micras- monomodo

1.9 Medios Inalámbricos

1.9.1 Radio ondas

Existen tres tipos de transmisiones de radio frecuencia: frecuencia única en baja potencia, frecuencia única en alta potencia y espectro amplio.

Las transmisiones por radio frecuencia de frecuencia única en baja potencia ofrecen transmisiones a muy cortas distancias, típicamente de 50 a 70 m (la distancia exacta depende de múltiples factores.) En este tipo de transmisiones no se requiere que el emisor y el receptor estén en línea de vista directa y manejan velocidades relativamente bajas. Las transmisiones hechas por este método son muy susceptibles a interferencias provocadas por ruidos en el pequeño rango de transmisión que manejan.

Las transmisiones por radio frecuencia única en alta potencia mantiene las características de su contraparte de baja potencia, con la excepción de que el área de cobertura es mucho más extensa.

Las transmisiones por espectro amplio o *spread spectrum* son menos susceptibles a interferencias y son más seguras que las de frecuencia única. El espectro amplio utiliza un ancho de banda mayor y saltos de frecuencia o secuencias de modulación directa. En los saltos de frecuencia, la información que se transmite salta de frecuencia en frecuencia por diferentes canales. En la secuencia de modulación directa, la información se divide en fragmentos muy pequeños que se transmiten simultáneamente por varios canales de frecuencia. Por estas características, el espectro amplio es muy difícil de interceptar por personas no autorizadas mientras

que para interceptar las transmisiones de frecuencia única, tan solo es necesario encontrar la frecuencia de transmisión de la señal.

Algunas de las aplicaciones en redes de las transmisiones inalámbricas por radio frecuencia son:

- Transmisión en LAN por banda delgada. Para utilizarla es necesario tener licencias para el uso de la frecuencia específica.
- Servicios de comunicación personal (PCS.) En banda delgada se utiliza para beepers y paginadores y mensajería en texto en dos sentidos. En banda ancha se utiliza para cámaras y teléfonos celulares.
- Dentro de la categoría de espectro amplio se encuentran las especificaciones 802.11a que transmite a velocidades de 54Mbps sobre una portadora de 5Ghz, 802.11b que transmite a 11Mbps sobre una portadora a 2.4Ghz y 802.11g que transmite sobre la misma frecuencia que la 802.11b pero a velocidades de hasta 54Mbps.

Véase la figura 1.12

1.9.2 Infrarrojos

Las transmisiones por infrarrojos se basan en la emisión y recepción de rayos infrarrojos, éstas son bastante rápidas (de 115Kbps hasta 4Mbps) y siguen aumentando su velocidad. Sin embargo, las distancias manejadas son sumamente reducidas, lo que limita esta tecnología al área de transmisiones entre laptops y a nivel personal únicamente. Hay una nueva especificación que promete velocidades de hasta 16Mbps, se llama VFIR (*Very Fast Infrared*) pero esta especificación aún no es una realidad.

Las comunicaciones por infrarrojos se hacen de manera directa y en línea de vista, el haz de luz infrarroja se dispersa en un ángulo de emisión amplio para facilitar la alineación entre el emisor y el receptor, pero esto debilita aún más la señal y consecuentemente la distancia de transmisión se acorta.

Véase la figura 1.12

1.9.3 Microondas

Las microondas son otro medio de transmisión que requiere de línea de vista directa y normalmente son difíciles de instalar y configurar. Las transmisiones por microondas se pueden hacer por medio de satélite y por medio de antenas en lugares muy elevados. Las transmisiones por microondas son susceptibles a interferencias causadas por condiciones atmosféricas. En el caso de las transmisiones por satélite y a causa de las grandes distancias que se cubren, pueden existir retrasos en las transmisiones que varían desde .05 hasta 5 segundos. Véase la figura 1.12

A pesar de las ventajas en comodidad de uso que ofrecen las transmisiones inalámbricas, éstas aún no tienen la tecnología para competir con las comunicaciones en LAN hechas por cable.

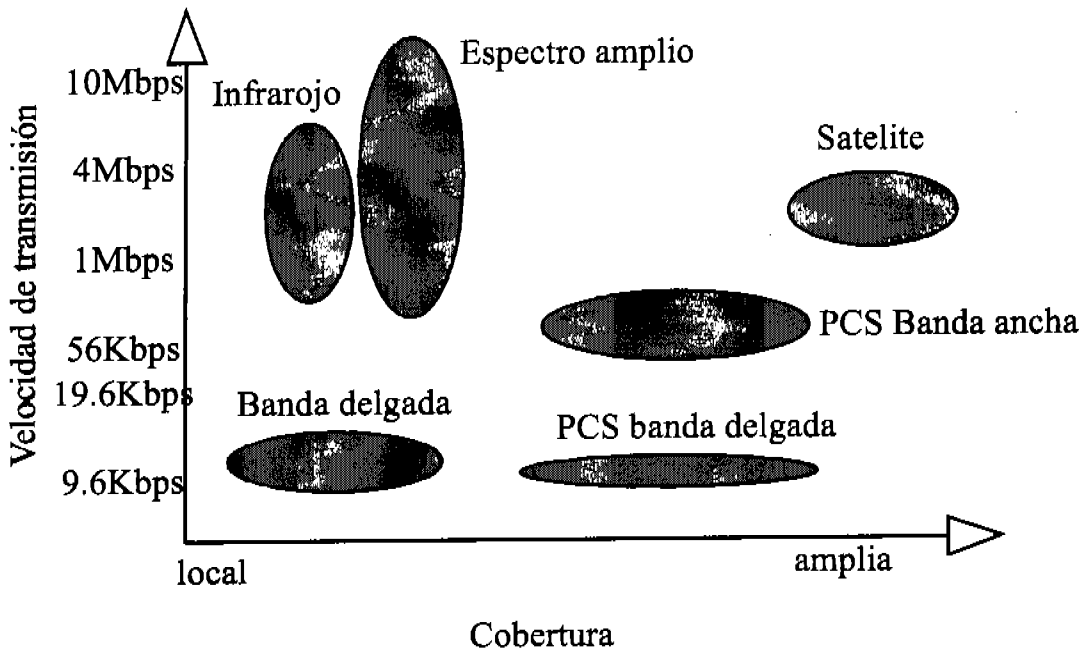


Figura 1.12 Velocidades de transmisión vs. cobertura de algunas aplicaciones inalámbricas

1.10 Conectores de Red

Existe una gran variedad de conectores asociados con diferentes medios de transmisión.

1.10.1 Conectores BNC

Los conectores BNC (*British Naval Connector, Bayonet Nelly Concelman o Bayonet Nut Connector*) se asocian con el cable coaxial y aunque no son tan populares como alguna vez lo fueron, aún se utilizan en ciertas redes. Los conectores BNC más comunes son: el conector "T", el conector de barril o "gusano" y el terminador. Además de encontrarse en algunas tarjetas de red y concentradores antiguos. Ver figura 1.13

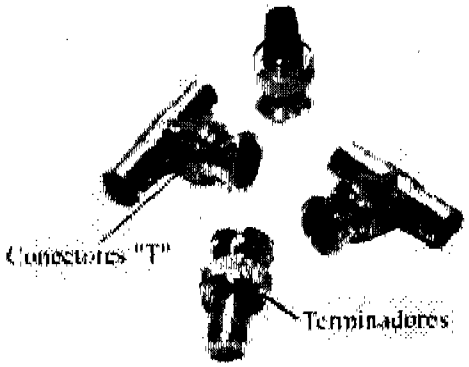


Figura 1.13 Conectores BNC

1.10.2 Conectores RJ-45

Los conectores RJ-45 (*Registered Jack* 4,5) son actualmente los más conocidos en el campo de las redes ya que son los que se emplean para la interconexión del cable par trenzado. Estos conectores se parecen a los conectores de telefonía ordinarios (RJ-11) con la diferencia de que los telefónicos son un poco más cortos y tan solo manejan 4 hilos. El RJ-45 conecta 8 cables. La figura 1.14 muestra algunos conectores RJ-45.

Figura 1.14 Conectores RJ-45

1.10.3 Conectores AUI

Los conectores AUI (*Attachment Unit Interface*) son conectores que se utilizan en *hubs*, *switches* e implementaciones con cable coaxial grueso. El AUI es un conector hembra de 15 pins. La figura 1.15 muestra un par de conectores AUI en un ruteador.

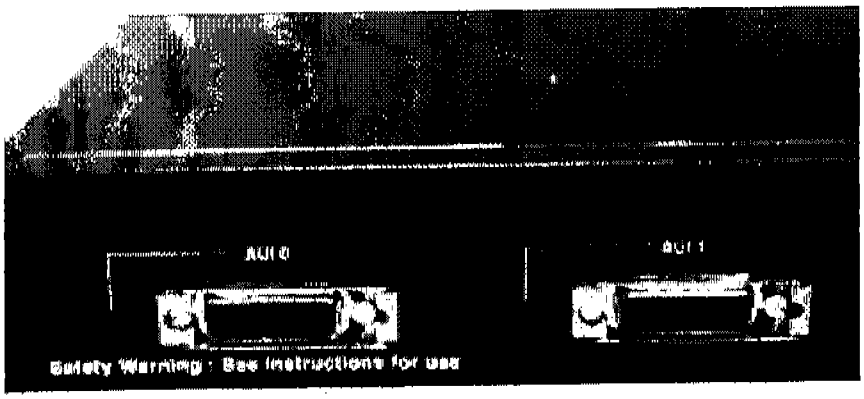


Figura 1.15 Conectores AUI en un ruteador

1.10.4 Conectores de fibra óptica

Hay una gran variedad de conectores para fibra óptica y varias formas de conexión: por medio de bayoneta, con seguro plástico, de jalar y empujar, etc.

La figura 1.16 muestra los conectores de fibra óptica más comunes.

Figura 1.16 Conectores de fibra óptica

1.11 Estándares 802.3 de la IEEE

Dentro de los estándares para redes definidos por la IEEE, el más popular es el 802.3 que regula el uso de varios sistemas basados en el estándar 802.3 original, *Ethernet*. El esquema nominativo de estos estándares es:

[velocidad][basebanda o banda ancha][distancia o tipo de cable]

Por supuesto que en *Ethernet* siempre se usa basebanda.

1.11.1 Estándar 802.3 10base2

El estándar 10base2 especifica velocidades de transmisión de 10Mbps y longitudes máximas de cable de 185m (la intención original es que fueran de 200m) utilizando cable coaxial delgado, conectores tipo "T" y terminadores de 50ohms. Este estándar especifica una topología bus en la que por lo menos uno de los extremos en cada segmento de cable debe estar debidamente aterrizado.

Las redes 10base2 permiten un máximo de cinco segmentos, de los cuales solamente tres pueden estar poblados, y cada uno de los segmentos poblados puede tener un máximo de 30 dispositivos conectados. 10base2 requiere una longitud mínima de cable de 0.5m. Ver figura 1.17

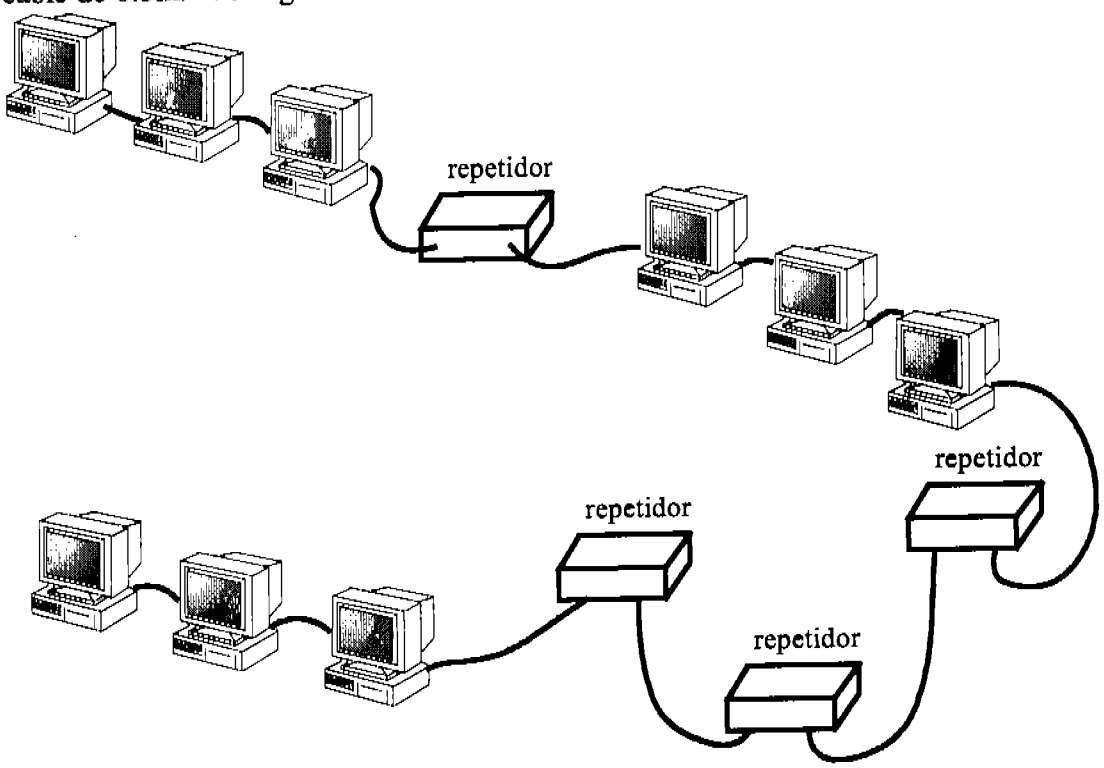


Figura 1-17 Regla 5-4-3 para coaxial delgado. 5 segmentos, 4 repetidores y 3 segmentos poblados

1.11.2 Estándar 802.3 10base5

Al igual que 10base2, 10base5 tiene una velocidad de 10Mbps y especifica una topología bus. 10base5 se desarrolló para proveer de un buen medio de transmisión como espina dorsal entre redes más pequeñas ya que utiliza cable coaxial grueso que permite distancias máximas por cable de 500m y tiene muy buena resistencia a EMI y crosstalk. El máximo número de dispositivos que se pueden conectar en un segmento de 500 metros en 10base5 es 100. Al igual que en 10base2, 10base5 permite sólo tres segmentos poblados de un máximo de 5 y cada segmento debe tener por lo menos un extremo aterrizado.

10base5 es más difícil de implementar que 10base2 ya que requiere de transceivers y vampiros como conectores. La distancia mínima en un cable bajo el estándar 10base5 es de 2.5m, mientras que la mayor distancia del conector al dispositivo es de 5 metros. Ver figura 1.18.

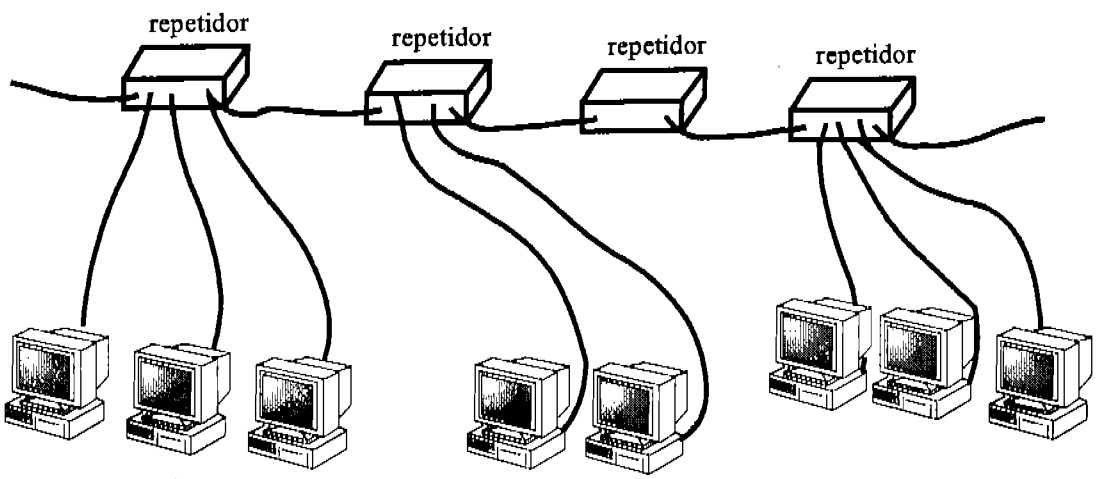


Figura 1.18 Regla 5-4-3 para coaxial grueso. 5 segmentos, 4 repetidores y 3 segmentos poblados.

1.11.3 Estándar 802.3 10baseT

10baseT es otra tecnología a 10Mbps con la diferencia que este estándar utiliza cable de par trenzado. Las redes 10baseT tienen un máximo de 100metros por segmento de cable y un mínimo de 90cm. En este tipo de redes puede haber hasta cinco segmentos con cuatro repetidores, pero a diferencia de las redes implementadas con cable coaxial, todos los segmentos pueden estar poblados.

El estándar para las redes 10baseT establece una conexión punto a punto entre las computadoras y un *hub* o *switch*, obviamente en topología estrella. Las redes 10baseT pueden implementarse utilizando par trenzado de categorías 3, 4 ó 5.

1.11.4 Estándar 802.3 10baseFL

Aunque éste no es estándar muy utilizado, es interesante mencionarlo ya que permite una comunicación a 10Mbps sobre un medio de... ¡Fibra óptica! Probablemente la única ventaja de este estándar es que permite transmisiones inmunes al EMI a grandes distancias (de hasta 2000m.)

1.12 *Fast Ethernet*, 802.3u

La gran mayoría de las aplicaciones de hoy en día requieren un ancho de banda mayor al ofrecido por los estándares a 10Mbps. Para satisfacer esta necesidad de velocidad, la IEEE ha desarrollado las especificaciones a 100Mbps dentro del estándar 802.3u de la cual existen tres variaciones:

1.12.1 Estándar 100baseTX

La primera y más ampliamente utilizada de las tecnologías definidas para *Fast Ethernet* es la 100baseTX. El estándar 100baseTX utiliza dos de los cuatro pares de alambres que ofrece el par trenzado UTP categoría 5 y puede utilizar par trenzado STP cuando se requiere de mayor inmunidad al EMI. 100baseTX utiliza transmisiones a 100Mbps sobre distancias máximas de 100m.

1.12.2 Estándar 100baseT4

100baseT4 también es una tecnología que permite transmisiones a 100Mbps sobre segmentos de cable par trenzado de hasta 100m de longitud. La gran diferencia con 100baseTX es que en este estándar se puede utilizar cable de categoría 3, 4 y 5 ya que el estándar define que se utilizan los 4 pares de alambres que conforman el par trenzado. Esta tecnología es muy útil, en especial en ambientes en donde ya se tiene la red tendida con uno de estos cables de par trenzado de categorías inferiores y no se desea sustituirlo.

1.12.3 Estándar 100baseFX

El estándar 802.3 100baseFX especifica transmisiones de 100Mbps sobre fibra óptica. 100baseFX puede utilizar tanto fibra óptica monomodo como fibra óptica multimodo. Este estándar tiene una longitud máxima por segmento de cable de 412 metros si se implementa en fibra óptica multimodo y de 10000m cuando se implementa sobre monomodo.

1.13 *Gigabit Ethernet*

Las nuevas tecnologías han permitido la incursión en velocidades de red del orden de 1 Gbps. Es posible implementar la *Gigabit Ethernet* utilizando tanto cable de

cobre como fibra óptica. Ésta última siendo, por supuesto, la más versátil. Los dos estándares que define la transferencia a 1 *Gigabit* por segundo son la 802.3z y la 802.3ab.

1.13.1 Estándar 802.3z

Dentro del estándar 802.3z se especifica la familia de estándares conocida como la 1000x. Ésta se compone de tres estándares: el 1000baseLX, el 1000baseSX y el 1000baseCX. Los estándares 1000baseLX y 1000baseSX se implementan sobre fibra óptica multimodo de 50 ó 62.5 micras de diámetro y utilizan señales por láser de onda larga y por láser de onda corta respectivamente. Además, las señales enviadas por láser de onda larga soportan el uso de fibra óptica monomodo.
En el estándar 1000baseCX se utiliza cable de cobre STP. Dado que se fuerza una señal demasiado rápida sobre el cobre, los efectos de interferencia se acentúan enormemente, por lo que 1000baseCX soporta distancias máximas de transmisión de tan sólo 25metros.

1.13.2 Estándar 802.3ab

El estándar 802.3ab especifica el uso de cable categoría 5 UTP para transferencia de datos a 1Gbps. Para lograr este ancho de banda se utilizan los cuatro pares de alambres del par trenzado; cada par transmite a una velocidad de 250Mbps.

1.14 Dispositivos de Red

Todas las redes computacionales requieren de dispositivos especiales que proveen conectividad y funcionalidad. Entender las funciones y diferencias básicas entre estos dispositivos es indispensable para una buena planeación e implementación de cualquier red ya que los requerimientos particulares de cada red se deben satisfacer utilizando los dispositivos adecuados en cada caso.

1.14.1 Repetidores

Conforme la señal viaja a través de un medio sufre los efectos de atenuación e interferencia, efectos que limitan la distancia de transmisión. Cuando se requiere que una señal viaje más lejos de lo que permite el medio de transmisión, se utiliza un repetidor. El repetidor regenera las señales llevándolas a niveles nominales y añadiéndoles potencia. Véase la figura 1.19

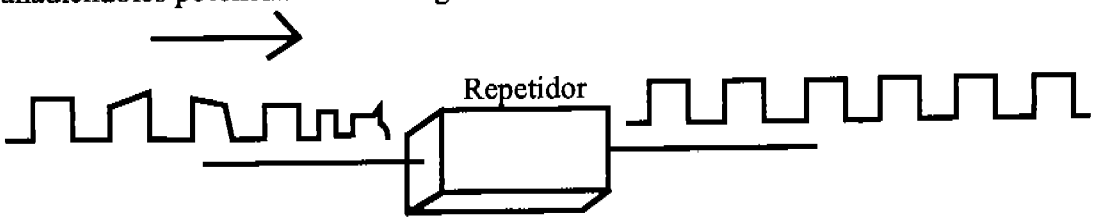


Figura 1.19 Repetidor

1.14.2 *Hubs*

Los *hubs* son dispositivos que centralizan las conexiones de las máquinas en una red. Éstos se emplean en redes que utilizan par trenzado en estrella física. Es posible interconectar varios *hubs* entre sí para crear redes más grandes.

Los *hubs* son dispositivos muy básicos, los cuales redirigen los paquetes recibidos por cualquiera de las máquinas conectadas a alguno de sus puertos, hacia todas las demás máquinas conectadas a todos sus demás puertos, sin importar el destinatario de la información. Esto hace de los *hubs* dispositivos ineficientes ya que sin importar el origen o el destino de un paquete, todas las computadoras conectadas lo reciben y por consecuencia, en cualquier momento dado, tan sólo una computadora puede estar enviando información en toda la red. Este método de transmisión crea invariablemente cuellos de botella en redes con mucho tráfico. Véase la figura 1.20

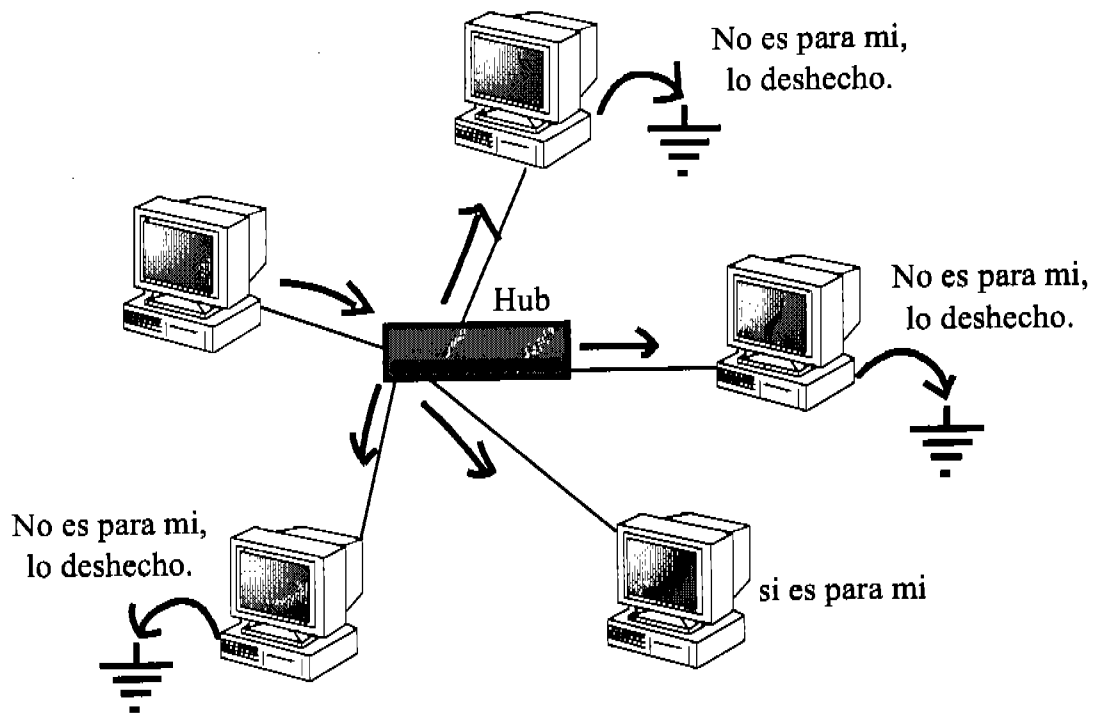


Figura 1.20 Funcionamiento de un *hub*

En su forma más básica lo único que hace un *hub* es proveer un camino para que las señales lleguen a su destino, un dispositivo así es un *hub* pasivo. Hoy en día es mucho más común encontrar *hubs* activos. Los *hubs* activos se caracterizan por regenerar las señales que reciben antes de reenviarlas al resto de las computadoras conectadas. Se puede pensar en un *hub* activo como un repetidor de múltiples puertos. Sin embargo, aún el *hub* activo no realiza ningún proceso de decisión o de revisión de errores sobre las señales que recibe y reenvía.

1.14.3 MSAU

El MSAU es el dispositivo que permite la implementación de un anillo lógico sobre una estrella física. Al MSAU (*Multistation Access Unit*) se le conoce por diferentes nombres: MSAU, SMAU, SAU y MAU. Todos estos nombres identifican a uno y al mismo dispositivo. El MSAU realiza la secuenciación necesaria para el *token passing* en las topologías *token ring*. Para que una red basada en *token ring* crezca más allá de la capacidad que el número de puertos de un MSAU lo permite, es posible interconectar dos o más MSAU's haciendo un ciclo con ellos por medio de sus puertos especiales RI *(ring in)* y RO (*ring out.*)

La figura 1.6 muestra un anillo lógico implementado en una estrella física por medio de un MSAU.

1.14.4 *Switches*

Al igual que los *hubs*, los *switches* son dispositivos centralizadores de conexiones en redes *Ethernet*, cada dispositivo en la red se conecta por medio de un cable de par trenzado a un diferente puerto en el *switch*. La diferencia entre un *hub* y un *switch* radica en la forma en que cada dispositivo maneja la información: mientras que el *hub* envía la información que recibe hacia todos los dispositivos de la red por cada uno de los puertos que tiene, el *switch* envía los paquetes de información que recibe tan sólo al dispositivo identificado como el destinatario de dicho paquete. Esto lo hace relacionando en una tabla en memoria las direcciones de los dispositivos con los puertos del mismo *switch* por los que se llega a tales dispositivos.

Al transmitir la información únicamente hacia el dispositivo al que va dirigida, el *switch* mejora el rendimiento de la red considerablemente. El *switch* realiza una interrupción por *hardware* entre los dos puertos de las máquinas que se están comunicando; en otras palabras, realiza una conexión punto a punto que conecta directamente a las dos máquinas. Al hacer esto, se reducen de manera muy importante el número de colisiones en la red ya que cada par de puertos puede mantener simultáneamente una transmisión entre sí, sin provocar colisión alguna con algún otro puerto. La única manera en que se pueden presentar colisiones al utilizar un *switch* es que dos o más máquinas traten de accesar a la misma máquina exactamente al mismo tiempo.

Mientras que al utilizar un *hub* el ancho de banda se dividía entre todos los usuarios, al utilizar un *switch*, cada puerto tiene de manera dedicada todo el ancho de banda que el dispositivo ofrece. Aprovechando la falta de colisiones entre dispositivos, un *switch* puede transmitir en modo *full duplex*, es decir que cada computadora puede enviar y recibir paquetes desde el *switch* al mismo tiempo. Una forma de ver esto es que, si la velocidad del *switch* es de 100Mbps, cada tarjeta que esté funcionando en full-duplex estará realmente manejando 200Mbps.

Existen tres métodos por los cuales un *switch* puede tomar la decisión de por qué puerto mandar la información: En tiempo real (*cut-through*), *cut-through* modificado (*fragment free*) y almacena y envía (*store and forward.*)

La figura 1.21 muestra la forma en la que un *switch* reenvía la información que recibe.

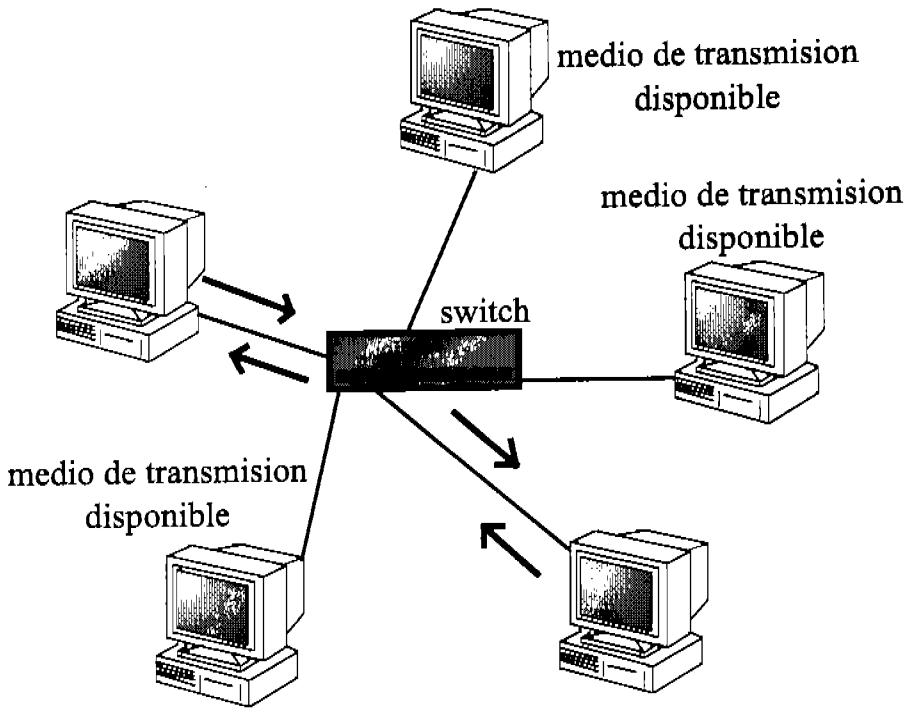


Figura 1.21 Funcionamiento de un *Switch*. Los datos sólo se envían al nodo de destino y no a todas las computadoras en la red.

1.14.5 *Bridges*

Los *bridges* se utilizan para dividir redes grandes en secciones más pequeñas. Para hacerlo, se coloca un *bridge* entre dos segmentos físicos de una red. El *bridge* relaciona las computadoras en cada segmento con su propia interfase conectada a ese mismo segmento e impide que los paquetes generados en un segmento con destino a una máquina del mismo segmento crucen hacia el otro segmento de la red. Si el paquete va dirigido a una computadora en el otro segmento de la red, entonces el *bridge* lo reenvía hacia ese segmento. La ventaja de segregar así una red es, por supuesto, que el tráfico de un segmento que no va dirigido a alguna computadora en el otro segmento no afecta a ambos segmentos y por lo tanto el rendimiento de red es mucho mejor que si todas las señales fueran recibidas por todas las computadoras.

Otra manera de ver a un *bridge* es como un *switch* de dos puertos, de hecho el funcionamiento lógico de ambos dispositivos es exactamente el mismo: proveer la capacidad total del ancho de banda a cada uno de sus puertos. Además de la diferencia en el número de puertos, el *switch* hace las interrupciones por *hardware*, mientras el *bridge* los hace por *software*. Véase la figura 1.22

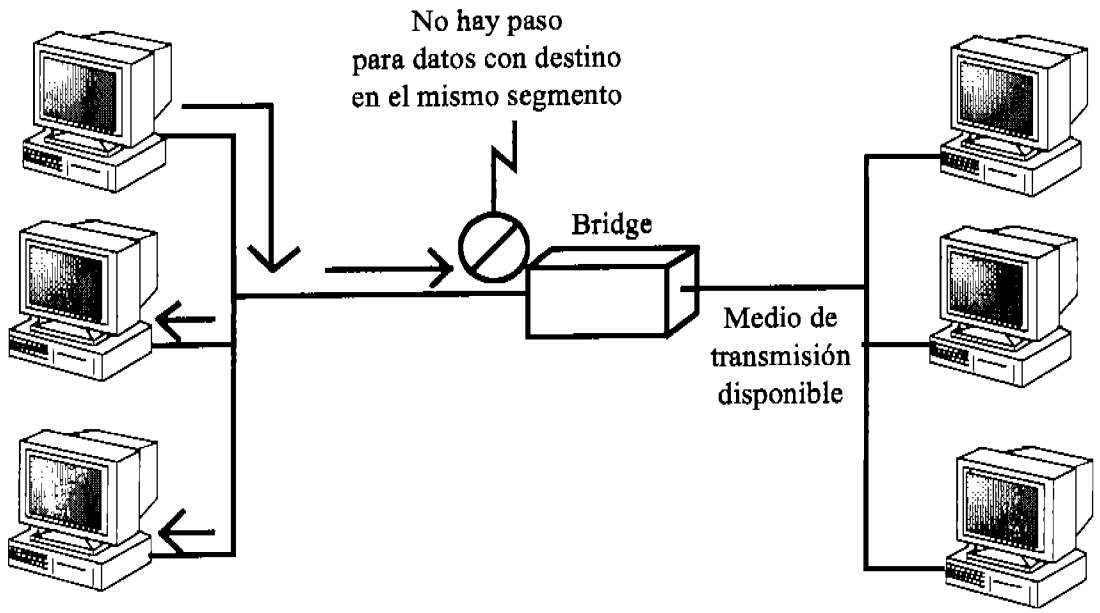


Figura 1.22 El *bridge* impide que datos dirigidos al mismo segmento pasen pero permite el paso a datos con destino en el otro segmento.

En las primeras versiones de *bridges*, era necesario configurar manualmente las direcciones físicas de los dispositivos conectados a cada puerto del *bridge*. Debido a que esto significaba teclear las direcciones de todos los dispositivos en el segmento de red correspondiente, este proceso se prestaba a que se cometieran muchos errores difíciles de detectar antes de que se presentara algún problema de conectividad. Hoy en día, ya casi no se utilizan los *bridges* puesto que para fines prácticos proveen la misma funcionalidad que un *switch* pero con menos puertos. La mayoría de los *bridges* actuales tiene la funcionalidad de construir la lista de dispositivos en cada segmento simplemente observando el tráfico en la red, a estos *bridges* se les llama *learning bridges*.

Un buen diseño requiere que las computadoras sean divididas en los dos segmentos de acuerdo a la regla 80/20 que dice que el 80% de las comunicaciones deben permanecer en el segmento local mientras que el 20% restante debe dirigirse hacia el otro segmento.

Un problema que se presenta en escenarios con más de un learning *bridge*, es el ciclo de búsqueda infinito. Este ciclo se presenta cuando un *bridge* recibe un paquete de información dirigido a un dispositivo inexistente, el *bridge* aprende que ese

dispositivo está en otro segmento y lo envía al otro *bridge* el que a su vez considera remoto el dispositivo y lo regresa al primer *bridge* y así sucesivamente en un ciclo virtualmente infinito. Para romper este ciclo, la IEEE definió el estándar 802.3d: Spanning Tree Protocol, el cual elimina las rutas redundantes hacia un mismo dispositivo de las tablas de los *bridges*.

Hay tres tipos de *bridges*: el *bridge* transparente, el *bridge* de ruta de origen y el *bridge* traductor.

El *bridge* transparente deriva su nombre del hecho que los demás dispositivos de la red no están al tanto de su existencia. Un *bridge* transparente no hace otra cosa más que bloquear o permitir el tráfico de datos basado en las direcciones físicas de los dispositivos en las redes que conecta.

El *bridge* de ruta de origen se utiliza en redes *token ring* y se llama así porque los paquetes que filtra tienen toda la ruta, desde el origen hasta el destino, especificada en el encabezado dentro de ellos mismos.

El *bridge* traductor se utiliza para convertir los datos de un formato a otro, por ejemplo de un formato de datos de *token ring* a *Ethernet*.

1.14.6 Ruteadores

Los ruteadores se utilizan para proveer conectividad entre diferentes redes. Un ruteador puede ser un dispositivo de *hardware* dedicado o una computadora con más de una interfase de red y el *software* apropiado para ruteo. La gran mayoría de los sistemas operativos de red (NOS) modernos incluyen la funcionalidad de ruteador.

El ruteador deriva su nombre del hecho de que provee una ruta para que los paquetes de información que recibe desde una computadora en una red, puedan llegar a su destino en otra computadora en una red distinta.

Cuando un ruteador recibe un paquete, lee el encabezado del paquete para determinar la dirección lógica de destino y a qué red pertenece dicha dirección. Una vez que ha determinado estos datos, busca en una lista interna (conocida como la tabla de ruteo) si tiene la ruta para llegar a dicha red y en caso de que la tenga, manda el paquete al siguiente nodo en esa ruta, que puede ser otro ruteador o directamente la red a la que se pretende alcanzar.
Los ruteadores, a diferencia de los *switches* toman sus decisiones basados en las direcciones lógicas y no las físicas de los dispositivos y en su tabla de direcciones buscan redes computacionales completas y no sólo dispositivos en particular.

La figura 1.23 muestra, a grandes rasgos, el funcionamiento de un ruteador.

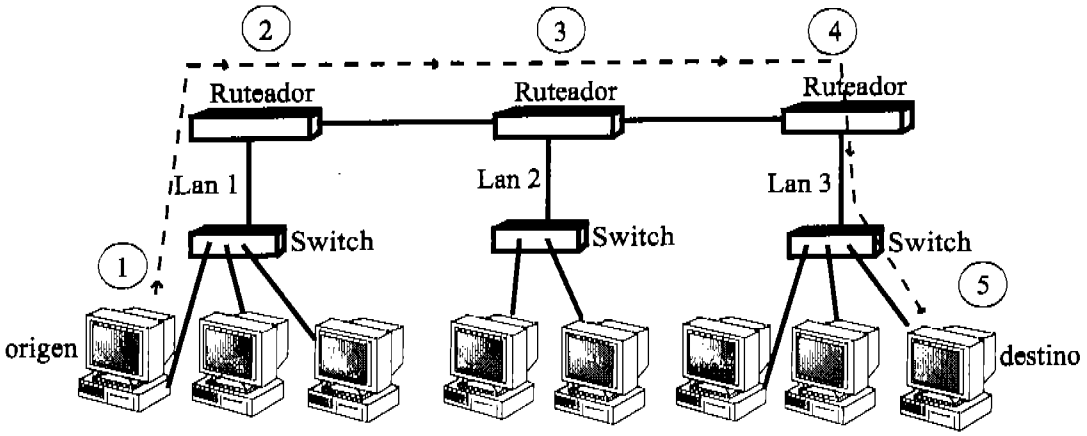


Figura 1.21.3 funcionamiento de un ruteador

En la figura 1.23 se pueden ver 5 pasos básicos en el trayecto de un paquete desde la computadora marcada como "origen" hasta la marcada como "destino" que ayudan a entender el funcionamiento de un ruteador:

1) La computadora origen genera el paquete a transmitir e incluye en él la dirección lógica del destino. Al determinar que la dirección de destino pertenece a otra red, la computadora origen envía este paquete al ruteador conectado a la LAN 1.
2) El ruteador de la LAN1 determina que la red a la que pertenece la computadora destino se encuentra en su tabla de ruteo. En esta tabla de ruteo dice que para alcanzar dicha red es necesario pasar por el ruteador conectado a la LAN2 así que lo envía a este ruteador.
3) El ruteador de la LAN2 identifica la red a la que pertenece la computadora destino en su propia tabla de ruteo. En esta tabla dice que para alcanzar la red de destino es necesario pasar a través del ruteador de la LAN3, por lo tanto el ruteador de la LAN2 envía el Paquete al ruteador de la LAN3.
4) El ruteador de la LAN3 recibe el paquete y determina que la red de destino se encuentra en su propia tabla de ruteo y que además esta directamente conectada a él. Por lo tanto lo envía al *switch* en su LAN.
5) El *switch* envía el paquete a la computadora cuya dirección coincide con la especificada en el paquete. Y el paquete llega a su destino.

Las tablas de ruteo juegan un papel muy importante en el proceso de determinar las rutas para enviar los paquetes en una red compuesta de varios segmentos o redes distintas. Por esto las tablas siempre deben de estar completas y actualizadas.
Hay dos formas básicamente en que un ruteador puede obtener la información que se necesita para la tabla de ruteo: a través del ruteo estático, en el que se deben introducir manualmente las rutas que llevan a las diferentes redes, y a través del ruteo dinámico, en que el ruteador automáticamente descubre y actualiza las rutas.

En el ruteo estático, dado que las rutas se introducen a la tabla de ruteo de manera manual, hay más probabilidades de errores, además de, que la configuración inicial y

la actualización de las rutas que cambian pueden ser muy demandantes en tiempo y esfuerzo. Por esto el ruteo estático se utiliza principalmente en ambientes muy pequeños en los que se cuenta con menos de 5 ruteadores. Para escenarios con mayor número de ruteadores siempre es más recomendable el ruteo dinámico.

En un ambiente de ruteo dinámico, los ruteadores utilizan protocolos de ruteo para comunicarse entre sí. Por medio de estos protocolos, los ruteadores transmiten información sobre sí mismos a otros ruteadores de manera que los demás ruteadores puedan construir sus tablas de ruteo de manera automática. Existen dos tipos de protocolos de ruteo dinámico: Los de vector de distancia (*distance vector*) y los de estado de conexión (*link state.*)

1.14.7 *Gateways*

Cualquier dispositivo que traduce datos de un formato a otro se conoce como un *gateway*. Algunos ejemplos comunes de *gateways* son: Un ruteador que convierte datos de un protocolo a otro, un *bridge* que convierte las señales de un sistema de red a otro, y hasta una aplicación de *software* que convierte entre dos formatos de presentación. Es difícil identificar el *gateway* como un dispositivo ya que en la mayoría de los casos el *gateway* no es un dispositivo por sí mismo, sino que es una funcionalidad integrada en otro dispositivo. El punto clave para identificar un *gateway* es que éste traduce tan solo la forma de la información, no la información misma. La figura 1.24 muestra un ejemplo de un *gateway*.

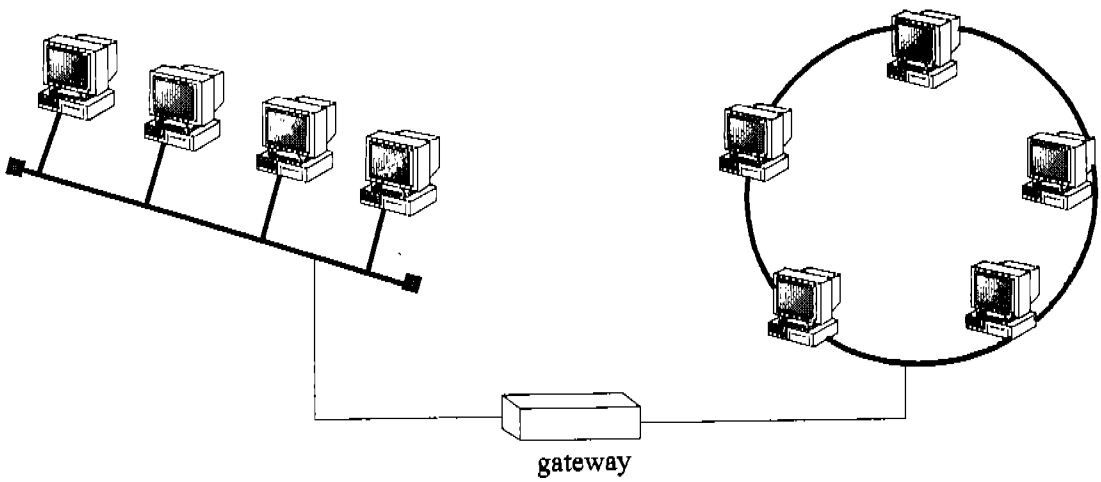


Figura 1.24 ***Gateway***

El término *default gateway* se presta a confusiones ya que no es lo mismo un *gateway* que un *default gateway*. El *default gateway* es la interfase por la cual se dirigen los paquetes de una red que tienen destinos en redes remotas.

1.14.8CSU/DSU

El Channel Service Unit / Digital Service Unit es un dispositivo que convierte las señales digitales que se utilizan en una LAN a señales utilizadas en WANs. Tal conversión es necesaria porque las señales utilizadas en LANs son diferentes a las que se utilizan en WANs aún si son digitales. El CSU/DSU se encuentra entre el punto de acceso provisto por la compañía de telecomunicaciones y la LAN y normalmente cuenta con un conector RJ-45 hembra. Muchos ruteadores incluyen la funcionalidad de un CSU/DSU.

1.14.9WAP

El *wireless access point* es el dispositivo que provee conectividad entre los dispositivos inalámbricos de una LAN y el resto de la red, normalmente alámbrica. La función de estos dispositivos es recibir una señal transportada por radio ondas y convertirla en el formato digital utilizado en la LAN.

1.14.10 Módem

Un módem, contracción de modulador-demodulador, es un dispositivo que convierte las señales digitales generadas por una computadora a señales analógicas que pueden viajar sobre líneas telefónicas. El módem en el extremo receptor de la línea, convierte la señal analógica recibida en la señal digital que la computadora entiende.

Los módems pueden manejar transmisiones de dos tipos, síncronas y asíncronas.

En las transmisiones síncronas, el módem que envía y el módem que recibe se coordinan en el tiempo de manera que el emisor pueda mandar (modular) varios paquetes de información al ritmo que el receptor los pueda ir convirtiendo (demodulando) y comprobando que han llegado sin alteraciones. En este método de transmisión, las dos computadoras involucradas en la comunicación se envían señales periódicas que indican el inicio y el término de una serie de paquetes y que están listas para recibir una nueva serie.

En las transmisiones asíncronas, cada paquete de información tiene una señal de inicio y de término dentro del paquete mismo, por lo que no es necesario que las computadoras se sincronicen para enviar y recibir la información. Sin embargo, como se puede apreciar en la figura 1.25 la relación de datos contra comandos de control de transmisión es más baja que en una transmisión síncrona. A pesar de esto, los módems asíncronos son los más populares.

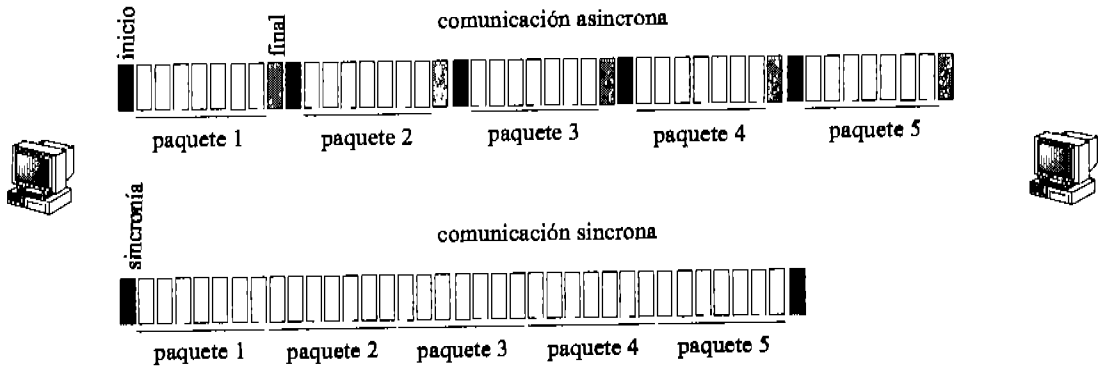


Figura 1.25 Comparación entre una transmisión síncrona y una asíncrona

La configuración de un módem es diferente para módems externos e internos. Para los módems internos, que son mucho más comunes hoy en día, el módem se debe configurar con una requisición de interrupción IRQ y una dirección de memoria de entrada/salida I/O.

Un factor que afecta la velocidad de transmisión de un módem es el UART (*Universal Asynchronous Receiver/Transmitter*) que es un circuito integrado que controla las comunicaciones seriales de una computadora. Véase la tabla 1.4.

Circuito UART	Velocidad (Kbps)
8250	9600
16450	9600
16550	115,200
16650	430,800
16750	921,600
16950	921,600

Tabla 1.4 Velocidades por modelo de UART

1.14.11 Tarjeta de red

Uno de los dispositivos más importantes en las redes es la tarjeta de red, por el simple motivo de que es la que permite que una computadora u otro dispositivo se conecte a la red.

Las tarjetas de red tienen diferentes funcionamientos para diferentes topologías. En el examen de certificación de Cisco tan sólo se toca el modo en que funciona una tarjeta de red para *Ethernet*. La tarjeta de red *Ethernet* puede tener diferentes velocidades que tienen que ver con la tecnología y las especificaciones de cada red, estas velocidades pueden ser de 10Mbps, 100Mbps ó 1000Mbps.

Según Cisco, una tarjeta de red realiza cuatro funciones básicas:

Las dos primeras funciones son fáciles de imaginar. La tarjeta de red convierte los datos a transmitir a señales transmisibles por el medio de transmisión y, por supuesto, convierte las señales que recibe a datos entendibles por la computadora.

La tercera función de una tarjeta de red es "escuchar el medio" (*Ethernet.*) En cada momento, una tarjeta de red debe saber si el medio de transmisión está libre, en caso de que la computadora necesite transmitir. Para determinar esto, la tarjeta de red hace un muestreo de su buffer constantemente. Si la tarjeta está transmitiendo en determinado momento, entonces el medio está siendo ocupado y no puede transmitir otro paquete en ese mismo momento. Si la tarjeta está recibiendo un paquete, sea el paquete destinado para esa computadora o no (recuérdese que en una red *Ethernet* todas las computadoras reciben todos los paquetes que se envían por la red y después determinan si pasan el paquete a su sistema operativo o lo derivan a tierra), entonces la red está siendo usada y no es posible transmitir un paquete de información en ese momento. Escuchar el medio requiere además de otro proceso, la detección de colisiones; Si entre el muestreo del medio que hacen las tarjetas de dos máquinas que quieren transmitir el medio está libre, ambas transmitirán al siguiente ciclo de sus procesadores provocando que las señales se sumen sobre el medio y no sea posible distinguir entre una señal y otra, a esto se le llama una colisión. Para detectar una colisión, la computadora que envía el paquete guarda una copia del mismo y al ponerlo en la red, lo recibe ella misma. Si el paquete tomado de la red es igual al paquete que se guardó entonces no hubo colisión, pero si los paquetes son distintos entonces hubo una colisión y la tarjeta entra en un algoritmo de espera semi-aleatorio basado en su dirección física para volver a transmitir. A este algoritmo se le conoce como *Backoff Algorithm.*

La última función de una tarjeta de red es determinar si un paquete en particular está dirigido a su propia computadora y en caso de que no sea así, derivarlo a tierra. Cada tarjeta de red tiene quemado en un PROM un número de identificación que, idealmente, es único en todo el mundo. Este número consiste en seis pares de dígitos hexadecimales de los cuales, los tres primeros identifican al fabricante y los demás los asigna el fabricante de manera consecutiva a cada una de sus tarjetas. Ésta es la dirección física de la computadora y se incluye en el campo de origen del encabezado de cada uno de los paquetes que viajarán por la red, además de que en cada paquete, en el campo de destino se incluye la dirección física que identifica a la tarjeta de la computadora destino.

A la dirección física de la tarjeta de red descrita anteriormente se le llama MAC (*Media Access Control.*)

Cuando una tarjeta de red en un entorno *Ethernet* recibe una señal, solamente traduce a datos el encabezado de ésta y compara la MAC en el campo de destino del encabezado contra su propia MAC, y así determina si traduce el resto del paquete o deriva a tierra todo el paquete.

1.15 Interconexión de Dispositivos por Medio de Par Trenzado

En el estudio de los medios de transmisión se observó que la razón del trenzado, del par trenzado es que; en cada par de alambres los electrones fluyan en distintas direcciones y por lo tanto los campos electromagnéticos generados se eliminen mutuamente, pero este diseño sería inútil si al conectar los dispositivos con el cable par trenzado, estos transmitieran por ambos hilos en la misma dirección. Por este motivo existen estándares en cuanto a la forma de colocar los conectores para la interconexión de dispositivos por medio de par trenzado.

Para interconectar dispositivos de la misma jerarquía como dos *switches* o dos ruteadores o dos computadoras directamente por medio de un cable, se utiliza un cable derecho (*straight-through*) mientras que para conectar directamente equipos de niveles jerárquicos adyacentes se utiliza un cable cruzado (*crossover.*)

En un cable derecho, el conector RJ-45 se conectan exactamente en el mismo orden todos los alambres en los dos extremos del cable. Véase la figura 1.26.

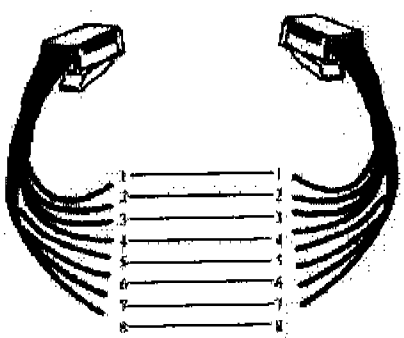


Figura 1.26 Cable derecho.

En el cable cruzado los alambres se cruzan en el orden que se muestra en la figura 1.27

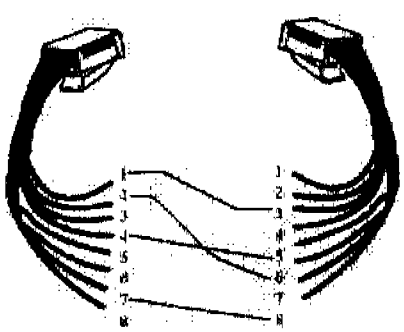


Figura 1.27 Cable cruzado.
Nota: por claridad sólo se ilustraron la mitad de las conexiones pero la otra mitad es simétrica.

Existen varias normas conocidas y aceptadas para conectar los diferentes dispositivos, y una de las más aceptadas en México es la 568.b en esta norma el orden de los colores en el RJ-45, viéndolo con la pestaña de seguridad hacia abajo y la abertura para los cables hacia enfrente y enumerando las terminales de izquierda a derecha (Véase la figura 1.28), es:

1. blanco naranja
2. naranja
3. blanco verde
4. azul
5. blanco azul
6. verde
7. blanco café
8. café

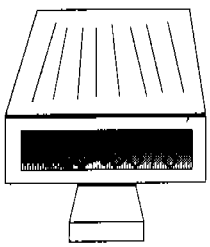


Figura 1.28 Orden de terminales

Existe un tipo de cable más que vale la pena mencionar, el rolled. A pesar de que el cable rolled no sirve para conectar ningún dispositivo en una red *Ethernet*, con este cable es posible conectar el puerto serial de comunicaciones (com) de una computadora a la consola de un ruteador o un *switch*. En el caso de ruteadores o *switches* Cisco, este cable se usa en conjunto con la aplicación de hyperterminal para conectarse al *hardware* de Cisco. En el cable rolled tan sólo se conectan en orden inverso las terminales de un extremo del cable mientras que en el otro extremo se conectan en el orden normal. Es decir, se cruzan los pines 1-8, 2-7, 3-6, y 4-5.

Capítulo 2

Modelos de Referencia y Protocolos IP

2.1 Introducción

Dado que este manual centra su atención en la certificación CCNA, es muy importante que se entiendan los diferentes modelos de referencia y que se entiendan según los ve Cisco.

Antes de discutir los modelos de referencia, es necesario entender el panorama general y saber porqué es importante aprender el manejo de redes Cisco. Las redes han tenido un crecimiento exponencial en los últimos 10 a 15 años y consecuentemente han tenido que evolucionar considerablemente tan solo para seguir proveyendo los servicios más básicos, como compartir impresoras o datos, con sus nuevas dimensiones, además para satisfacer las nuevas demandas que la misma tecnología impone, tales como las videoconferencias. En esta nueva estructura de redes se han tenido que resolver principalmente dos problemas: el primero es que ahora queremos compartir recursos de red con personas que se encuentran en áreas remotas por lo que es necesario conectar varias redes juntas, y el segundo problema es que dado que las redes han ido creciendo paulatinamente, llega el momento en que la congestión del tráfico en la red alcanza proporciones devastadoras, la solución a estos problemas es dividir la red en varias redes menores pero uniendo más redes en un mismo sistema que provea comunicación entre ellas. Unir redes mientras se dividen; es paradójico pero posible a través del manejo de redes.

En este capítulo se trata el manejo de redes además de los modelos de referencia que permiten un acercamiento por capas, de cómo deben de ocurrir las comunicaciones entre computadoras y entre redes. Por último se ve a detalle el modelo de referencia DoD y los diferentes protocolos que funcionan en cada una de sus capas.

2.2 Dominios de Colisión y Dominios de *Broadcast*

Las transmisiones en una red tipo LAN se pueden dividir en tres tipos basados en el destinatario de los datos: *unicast*, *multicast* y *broadcast*.

En una transmisión *unicast*, el destinatario es una sola computadora específica para la cual se conoce la dirección física y dicha dirección se incluye en el encabezado del paquete mismo. En una transmisión *multicast*, existen varios destinatarios para un mismo paquete. Estos destinatarios están dados de alta en un grupo que contiene una lista de suscripción con sus direcciones físicas. Al mandar un paquete a este grupo, se dirige una copia del mismo a cada dirección en la lista de suscripción. En una transmisión del tipo *broadcast*, los destinatarios para el paquete de datos son absolutamente todos los dispositivos en la red. En una transmisión *broadcast*, el paquete lleva una dirección especial en el encabezado, esta dirección reemplaza a la MAC que se pondría en una transmisión *unicast* y significa "Todos los dispositivos en la red" esta dirección es ff:ff:ff:ff:ff:ff en hexadecimal.

En la figura 2.1 se muestran las transmisiones *unicast*, *multicast* y *broadcast*.

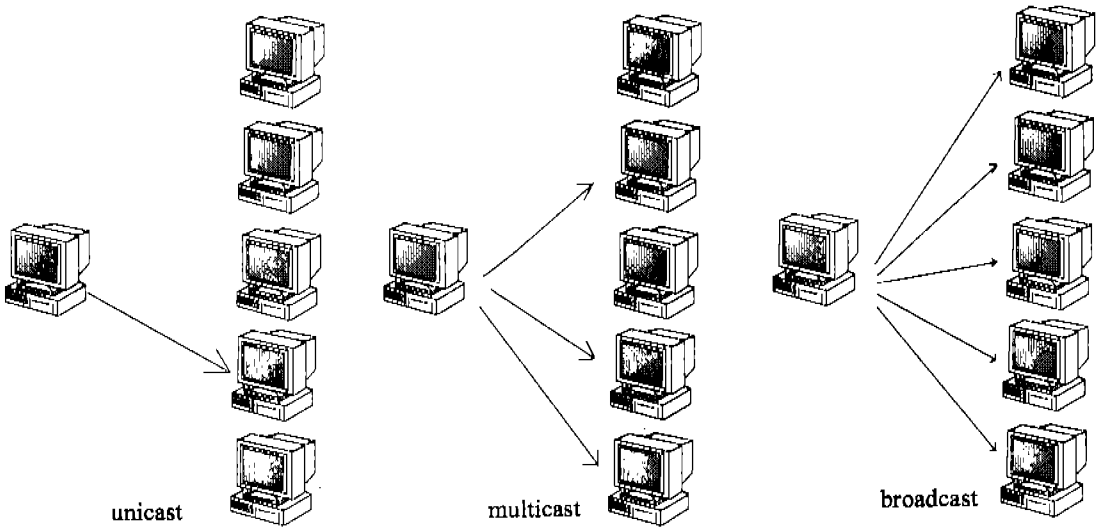


Figura 2.1 ***Unicast, Multicast* y *Broadcast***

Al hecho de dividir una red en redes menores para disminuir el tráfico se le llama segmentar la red, y esto puede ser logrado utilizando ruteadores, *switches* y *bridges*.

Un dominio de *broadcast* es, por lo tanto, el conjunto de todos los dispositivos en una red que reciben todas las transmisiones *broadcast* en ese segmento, es decir todos los paquetes cuya dirección de destino en sus encabezados sea ff:ff:ff:ff:ff:ff y procedan del mismo segmento de red. Esta definición sería redundante con la definición de *broadcast* si no fuera porque los ruteadores además de unir diferentes redes también rompen los dominios de colisión. En otras palabras, aunque un ruteador sirve para unir dos o más redes para que exista conectividad entre ellas, éste mantendrá las diferentes redes en segmentos distintos y con distintos dominios de *broadcast*.

Un dominio de colisión es, análogamente, el conjunto de dispositivos que al ingresar una señal a la red exactamente al mismo tiempo, producirán una colisión de datos. Tómese por ejemplo el diagrama de la figura 2.2

En dicha figura se muestra el esquema de una red dividida en tres sub-redes: una implementada con un *switch*, otra implementada con un *hub* y la tercera con un *bridge* y dos *hubs*.

Las tres máquinas en la red implementada con el *switch* pueden accesar a su propio segmento al mismo tiempo sin provocar una colisión (recuérdense las características del *switch*)[1] por lo tanto en esta sub-red hay por lo menos cuatro dominios de colisión (tres para las computadoras y uno para el ruteador.) De hecho, cada interfase de un *switch* tiene su propio dominio de colisión. Sin embargo, todos los

[1] En la página 36 se discuten las características de un switch.

dispositivos conectados a un *switch* pertenecen al mismo dominio de *broadcast* ya que un mensaje dirigido a "Todos los dispositivos" se transmite por todas las interfases del *switch*.

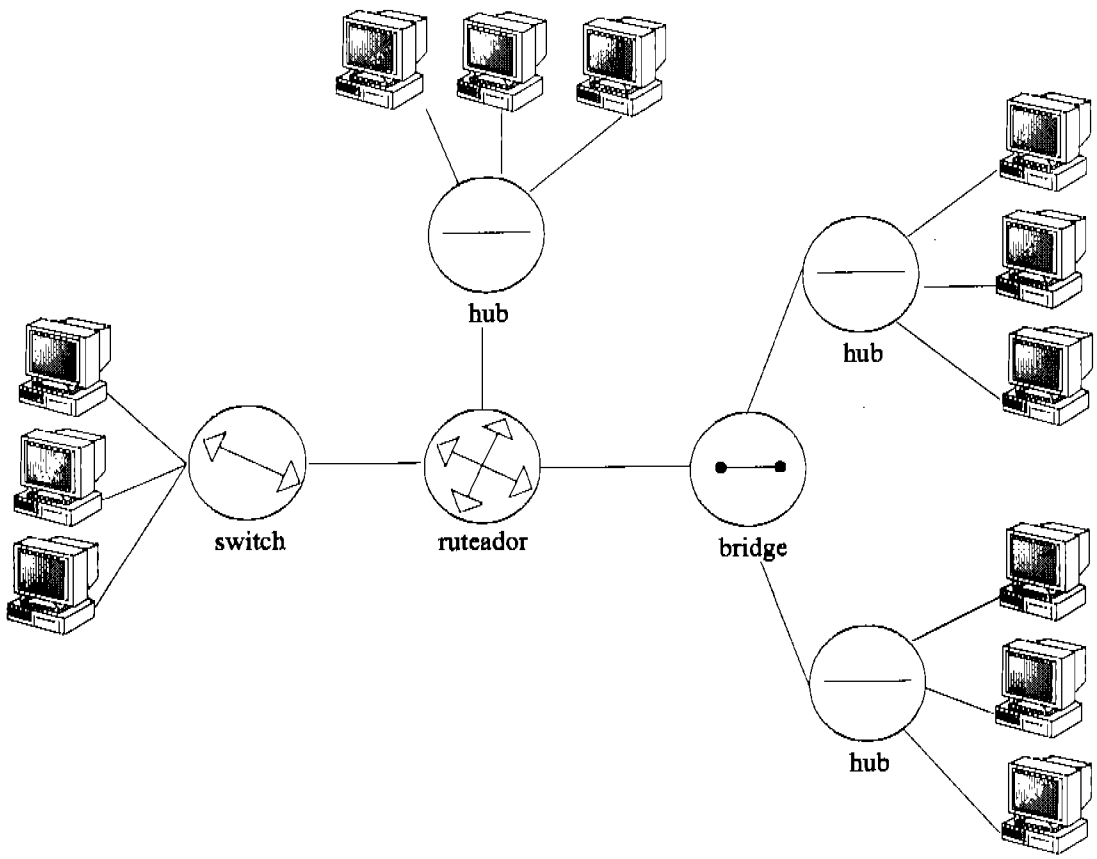


Figura 2.2 Dispositivos con distintos dominios de colisión y dominios de *broadcast*.

Entonces en la sub-red del *switch* existe un dominio de *broadcast* pero tantos dominios de colisión como puertos tenga el *switch*.

En la sub-red de arriba el *hub* tiene un solo dominio de *broadcast* porque todo paquete dirigido a todos los dispositivos de la red se dirige por todos los puertos del *hub*. Para ser precisos, cualquier paquete se dirige por todos los puertos del *hub*[2] sin importar el destinatario y esto define también que esta red tenga un solo dominio de colisión.

En la red de la derecha, compuesta por el *bridge* y los dos *hubs*, cada puerto del *bridge* tiene un dominio de colisión pero todos los puertos del *bridge* están en el

[2] Véanse las características de un *hub* en la página 35.

mismo dominio de *broadcast*[3]. Esto, por supuesto, quiere decir que la sub-red en cuestión tiene tres dominios de colisión pero sólo un dominio de *broadcast*.

Considerando la red desde el ruteador, cada una de las tres derivaciones tiene un dominio de colisión distinto que a su vez puede ser subdividido como en el caso del *switch* o el del *bridge* pero además, cada una de las interfases del ruteador tiene un dominio de *broadcast* distinto.

Es importante enfatizar que, a excepción de la configuración de VLANs con *switches*, el único dispositivo capaz de dividir los dominios de *broadcast* es el ruteador. Y lo hace de manera predeterminada.

2.3 Modelos de Referencia

Cuando nacieron las redes computacionales, las computadoras típicamente se podían comunicar solamente con computadoras del mismo fabricante y entonces se podían encontrar, por ejemplo, compañías que utilizaban ya fuera una red DECnet o una IBM pero no ambas juntas. A finales de los 70s la ISO (*International Standarization Organization*) creó el modelo de referencia OSI (*Open Systems Interconection*) con la intención de regular la interconexión de sistemas de cómputo de diferentes fabricantes.

El modelo OSI es el más importante de los modelos para redes. Este modelo norma la comunicación desde una aplicación en una computadora, a través del medio de conexión hasta la aplicación en otra computadora. El modelo OSI divide esta trayectoria en capas.

Las ventajas del modelo OSI son en concepto las mismas que las de cualquier modelo de referencia por capas. El propósito principal de estos modelos, en especial del modelo OSI, es permitir a diferentes fabricantes de diferentes productos en el campo de la tecnología de la información ínter operar por medio de la comunicación por redes. Otras buenas razones para utilizar los modelos jerárquicos de referencia son: permitir el desarrollo de *software* y *hardware* compatible entre múltiples fabricantes, permitir la comunicación entre varios tipos de redes, limitar los cambios de desarrollo a una sola capa del modelo de modo que dichos cambios no afecten a las demás capas y por lo tanto el desarrollo pueda ser modular, e identificar capas específicas en el modelo con los problemas en las redes, a la vez cada capa tiene ciertos protocolos, procesos y dispositivos relacionados a ella, de modo que se facilita la resolución de problemas.

[3] Véanse las características de un *bridge* en la página 37

2.4 Modelo Jerárquico de Tres Capas de Cisco

La mayoría de las personas han tenido de alguna u otra forma algún acercamiento a las jerarquías. Es a través de la jerarquía que entendemos a dónde pertenecen las cosas, cómo funcionan las cosas entre sí y que funciones tiene cada cosa. La jerarquía muchas veces divide modelos complejos en sistemas más ordenados y fáciles de entender. En el mundo del diseño de redes, la jerarquía ofrece muchas de las ventajas que ofrece en otras áreas de la vida.

El modelo jerárquico de Cisco define qué áreas en las redes deben realizar ciertas funciones y al utilizarse correctamente, hace las redes más predecibles y estables. Cisco define tres capas jerárquicas, las cuales pueden ser muy útiles al diseñar, implementar y mantener una red, que a la vez sea capaz de expandirse y tenga una excelente relación entre costos y eficiencia. Las tres capas del modelo jerárquico de Cisco son: *Core*, *Distribution* y *Access*. Véase la figura 2.3

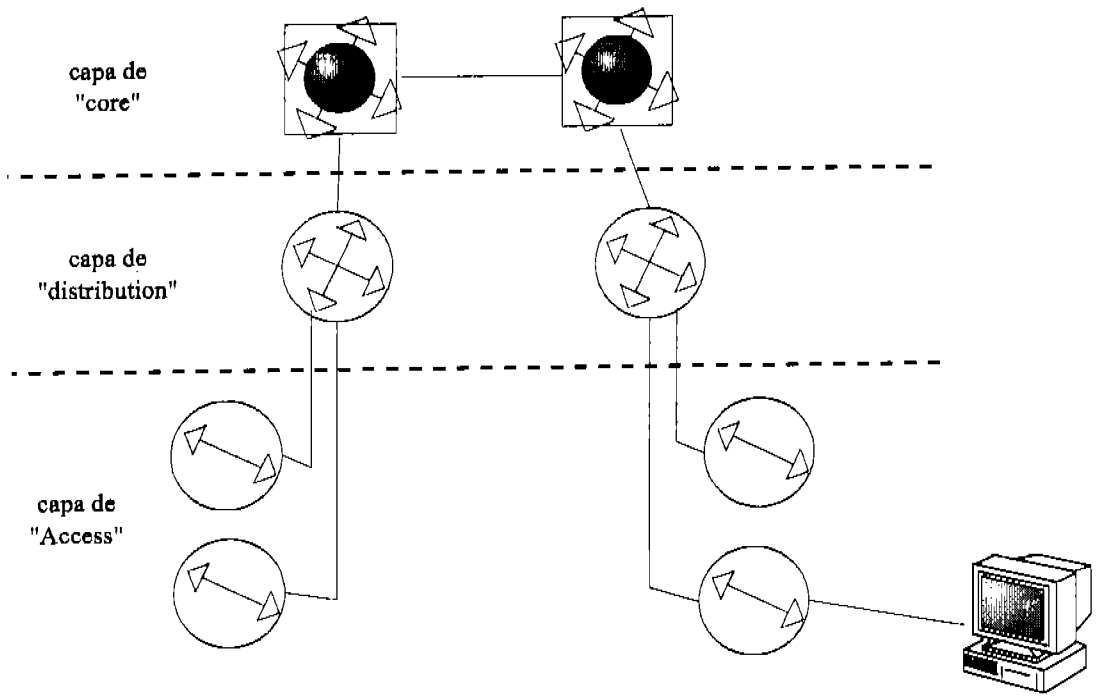


Figura 2.3 Modelo Jerárquico de Cisco. En la capa superior, *Core*, se muestran dispositivos del tipo *Frame Relay*, en la capa de distribución se muestran ruteadores y en la capa de acceso se muestran computadoras y *switches*. Sin embargo, hay que tener presente que los dispositivos mostrados son característicos de estas capas pero no necesariamente siempre pertenecen a ellas.

Cada una de las capas tiene funciones específicas. Sin embargo, estas capas son lógicas y no necesariamente se refieren a dispositivos físicos en particular. Un dispositivo puede estar relacionado con una sola capa pero también es posible encontrar un mismo dispositivo en más de una capa o múltiples dispositivos conviviendo en una misma capa.

2.4.1 Capa de *Core*

La capa de *core* es la capa principal de la red. En la cima de la jerarquía, la capa de *core* es responsable de transportar grandes cantidades de tráfico de manera confiable y rápida. El tráfico en la capa de *core* es tráfico común a la mayoría de los usuarios de la red (aunque los paquetes de cada usuario se procesan en la capa de *distribution* y solo se transmiten a la capa de *core* si es necesario.) La capa de *core* normalmente es el *backbone* o espina dorsal de la red, por lo que un fallo en esta capa puede afectar negativamente a todos los usuarios de la red. En esta capa es muy importante tener tolerancia a fallos.

Es fácil imaginarse que la capa de *core* maneja grandes volúmenes de tráfico, por lo que la velocidad y el tiempo de reacción son elementos de gran importancia en esta capa. Dada la funcionalidad de la capa de *core* hay ciertas consideraciones que hay que tener para esta capa al diseñar una red: para empezar es necesario evitar cualquier práctica en esta capa que resulte en un ralentizamiento del tráfico en la red, por ejemplo usar listas de acceso o ruteo entre VLANs o realizar cualquier filtrado de paquetes; es bueno también evitar que las decisiones de acceso a grupos de trabajo se hagan en esta capa; también hay que evitar en la medida de lo posible expandir esta capa conforme crece la red. ¡El propósito de esta capa es transmitir datos lo más rápidamente posible! Así que no es buena idea poner traba alguna al flujo de datos en la capa de *core*.

Por otro lado, hay cosas muy recomendables que hacer al diseñar esta capa de red como considerar una alta confiabilidad y tiempos de reacción reducidos, un buen ejemplo es utilizar FDDI o *Fast Ethernet* con rutas redundantes que proveen tolerancia a fallos y al mismo tiempo altas velocidades. Seleccionar protocolos de ruteo con tiempos de convergencia más cortos también es algo muy recomendable en esta capa.

2.4.2 Capa de *Distribution*

La capa de *distribution* también es conocida como la capa de grupos de trabajo y es el medio de conexión entre las otras dos capas en el modelo de Cisco. Las funciones principales de la capa de *distribution* son el proveer ruteo, filtrado, y acceso a diferentes WANs además de determinar cómo los paquetes pueden accesar la capa de *core* si es necesario. Esta capa se encarga de determinar la manera más rápida de satisfacer requisiciones de red.

La capa de *distribution* es el mejor lugar para implementar políticas de operación en la red.

Algunas acciones generalmente se deben realizar en esta capa: tales como ruteo; filtrado utilizando listas de acceso; implementación de seguridad y políticas de red,

incluyendo NATs y firewalls; establecimiento de protocolos de ruteo; definición de VLANs y ruteo entre ellas; determinación de dominios de *broadcast* y de *multicast*. Como regla general, las funciones que deben evitarse que realice esta capa son aquellas que específicamente se relacionan con alguna de las otras dos capas del modelo.

2.4.3 Capa de *Access*

La capa de *access* controla el acceso de usuarios y grupos de trabajo a recursos de red. A la capa de *access* también se le conoce como la capa de escritorio. La mayoría de los recursos que un usuario necesita, normalmente se encuentran en la red local por lo que este tráfico no es manejado por la capa de *distribution*.

Una buena planeación incluye en la capa de *access* las siguientes funciones:

- Control y políticas de acceso a nivel de red local (muchas veces continuando desde la capa de *distribution*.)
- Segmentación. Es decir, la creación de diferentes dominios de colisión.
- Conectividad hacia la capa de *distribution*.

Ethernet es una tecnología que normalmente se encuentra en la capa de *access*.

2.5 Modelo OSI

Una de las funciones más importantes de las especificaciones del modelo OSI es regular la transmisión de datos entre computadoras dispares. Por ejemplo, gracias a los estándares definidos por el OSI, una computadora Unix puede intercambiar datos con una PC o con una Mac.

Al igual que el modelo jerárquico de Cisco, el modelo OSI no es un modelo físico, sino una serie de normas y estándares que los desarrolladores pueden usar para crear e implementar aplicaciones de red. También es un modelo para crear e implementar estándares de red, dispositivos y esquemas de interrelación en redes.

El modelo OSI se divide en siete capas, que a su vez forman dos grupos: las capas superiores, que se encargan de la comunicación entre aplicaciones y la comunicación de las aplicaciones con los usuarios, y las capas inferiores, que definen la forma en que los datos se transmiten por la red de una computadora a otra.

Las siete capas del modelo OSI son:

- Capa 7-*Application* (Aplicación)

- Capa 6-*Presentation* (Presentación)
- Capa 5-*Session* (Sesión)
- Capa 4-*Transport* (Transporte)
- Capa 3-*Network* (Red)
- Capa 2-*Data-link* (Enlace de Datos)
- Capa 1-*Physical* (Física)

De las cuales aplicación, presentación y sesión son las capas superiores y; transporte, red, enlace de datos y física son las capas inferiores. Otra manera de referirse a las capas del modelo OSI es enumerándolas, siendo siempre la capa física la capa uno y la capa de aplicación la capa siete.

Una forma muy conocida para recordar los nombres de las siete capas del modelo es utilizar las iniciales de la frase en inglés "*All People Seem To Need Data Proccessing*".

2.5.1 Capa 7- Aplicación

En la capa de aplicación se encuentran los procesos necesarios para las aplicaciones que requieren servicios de red. Cabe aclarar que en esta capa no residen las aplicaciones en sí, sino los procesos que las aplicaciones necesitan para usar los recursos de red. Hecha la anterior aclaración, se estipula la excepción: las aplicaciones que inherentemente son aplicaciones para el uso de la red sí radican en esta capa. Algunos ejemplos de aplicaciones que radican en la capa de aplicación son FTP, SMTP y POP.

2.5.2 Capa 6- Presentación

En la capa de presentación se realiza la transformación del formato de los datos, de formatos que el usuario comprende (sonido, imágenes, texto en pantalla) a formatos que la computadora puede manejar (.wav, .jpeg, .txt.) Además de los servicios de traducción de formatos, en esta capa se hace la compresión de archivos y la encripción de datos. Esta capa se encarga de transformar archivos con las siguientes extensiones: PICT, TIFF, JPEG, MIDI, MPEG, Quick Time y RTF.

2.5.3 Capa 5- Sesión

En la capa de sesión se lleva a cabo el control de diálogos. En otras palabras, es en esta capa que se establecen, se manejan y finalmente se terminan las sesiones entre entidades de la capa de presentación. La capa de sesión mantiene también los datos de diferentes aplicaciones separados para mejorar el rendimiento de la computadora. También aquí se provee el diálogo entre dispositivos y nodos.

2.5.4 Capa 4- Transporte

La primera de las capas inferiores es la capa de transporte, esta capa provee la conexión de punto a punto entre el origen y el destino de los datos para que la comunicación pueda llevarse a cabo. La forma de entrega de los paquetes en la red puede ser confiable o no confiable y eso se define en esta capa. En esta capa también se lleva a cabo la corrección de errores y la retransmisión de los datos que se han perdido en la transmisión.

La capa de transporte es responsable de proveer mecanismos para multiplexar aplicaciones de las capas superiores y establecer y terminar circuitos virtuales de conexión.

La capa de transporte puede ser orientada a la conexión y no orientada a la conexión dependiendo de los protocolos utilizados. Sin embargo, para propósitos del examen, tan sólo se discute la parte orientada a la conexión.

Al hablar de una transmisión orientada a la conexión, implícitamente se está diciendo que es una comunicación confiable y que se utilizarán aknowledgments (acuses de recibo), secuenciación y control de flujo. Por medio de estas herramientas se logra lo siguiente:

- El dispositivo destino envía un *Acknowledgment* al origen al recibir los segmentos enviados.
- Cualquier segmento para el cual el emisor no recibe un aknowledgment es retransmitido.
- Los segmentos son reordenados por medio de las etiquetas de secuenciación en el extremo receptor.
- Los paquetes se envían evitando congestión, sobrecargas y pérdida de datos.

El control de flujo permite asegurar la recepción exitosa de los datos en el dispositivo destino. Hay un juego que se llama conejo gordo en el que el participante se coloca un malvavisco en la boca y dice "un conejo gordo", se coloca otro malvavisco y dice "dos conejos gordos", tres malvaviscos... 20 malvaviscos... 38 malvaviscos; "treinta y ocho conejos gordos" y así sigue hasta que no se le entiende lo que dice. Después de que el jugador establece su record, el juez le dice que puede ya comerse los malvaviscos que tiene en la boca, pero el jugador no puede hacerlo y termina por escupirlos todos. El control de flujo previene que la computadora origen sature los buffers de la computadora destino, y dado que los buffers requieren de espacio para mover sus datos y permitir la realización de procesos, al no haber espacio disponible, dicha saturación resulta en la pérdida de los datos contenidos en el buffer en ese momento.

Existen dos tipos de control de flujo: *buffering* y *windowing*. En el *buffering*, la computadora destino manda un mensaje de parada cuando el buffer está lleno y hasta que termina de procesar la información en el buffer manda un mensaje de reinicio, el cual está esperando la computadora origen para enviar más paquetes. En la transmisión confiable, los paquetes se deben recibir exactamente en el mismo orden en que se envían o toda la transmisión se pierde. La manera de resolver este problema es enviando un *Acknowledgment* por cada paquete recibido. Esto significa que al utilizar *buffering* en transmisiones confiables, la computadora origen tiene que esperar un *Acknowledgment* antes de enviar cada paquete y para poder enviar el *Acknowledgment*, la computadora destino debe de procesar el paquete anterior que recibió. Mientras la computadora destino procesa el último paquete recibido, ¡la computadora origen está esperando! Esta situación aunada al tráfico excesivo que representa mandar un acuse de recibo por cada paquete recibido hacen que el *buffering* solo se utilice en aplicaciones muy específicas.

Dado que hay tiempo desperdiciado en la transmisión desde que el destino recibe el paquete hasta que origen recibe el *Acknowledgment*, el emisor aprovecha este tiempo para transmitir más datos. A la cantidad de segmentos de información que la máquina origen transmite mientras recibe un *Acknowledgment* se le llama *windowing*. En una transmisión que utiliza este método solamente se emite un *Acknowledgment* por cada ventana. Véase la figura 2.4

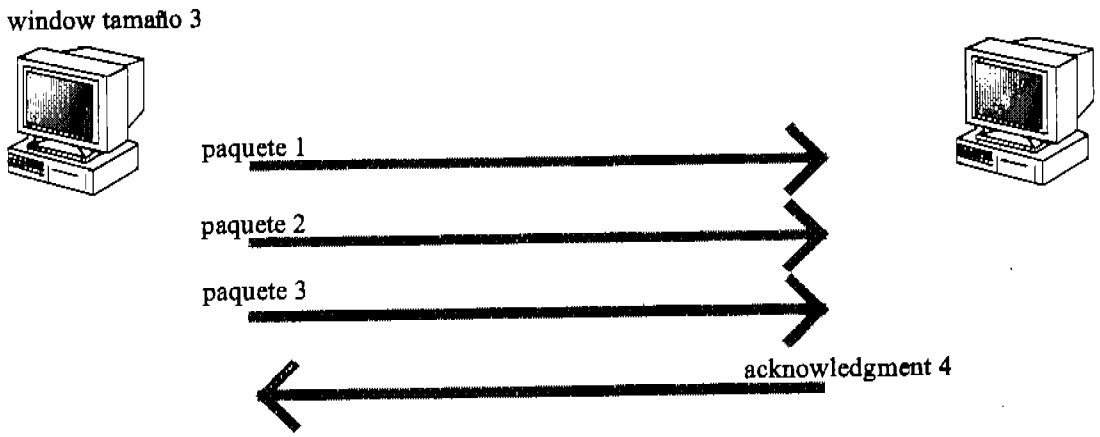


Figura 2.4 Transmisión por *window*. En este ejemplo, el tamaño de la ventana es de tres paquetes, lo que significa que mientras la computadora destino procesa el primer paquete, la computadora origen manda otros dos paquetes. Al terminar de recibir el tercer paquete, la computadora destino emite un *Acknowledgment* positivo. Es decir, un paquete que dice "lista para recibir el cuarto paquete"

En las transmisiones confiables se utiliza el *Acknowledgment* positivo. El *Acknowledgment* positivo le permite a la computadora destino especificar el paquete en particular que debe recibir a continuación, sea éste algún paquete que se recibió dañado o el primer paquete de la siguiente ventana. Véase la figura 2.5

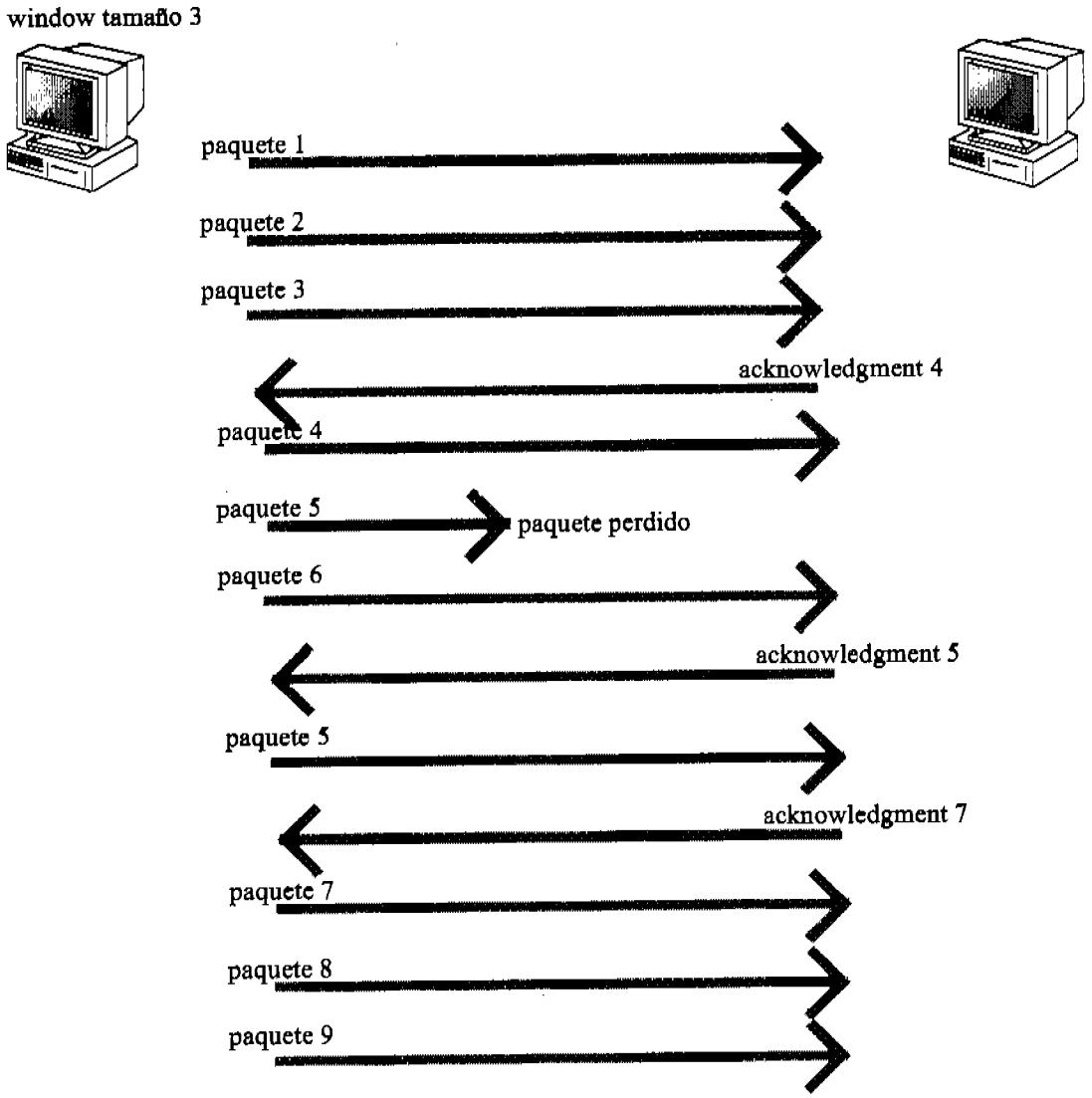


Figura 2.5 ***Acknowledgment*** **positivo.**

2.5.5 Capa 3- Red

En la capa de red o *network* se provee la forma en que los paquetes que viajan por la red encuentren su destino. En esta capa se establece el direccionamiento lógico de los dispositivos en la red local y remota de manera que se puede ubicar un dispositivo en particular en todo el mundo. El ruteo se hace aquí, es decir que en esta capa se determina el camino que los paquetes seguirán para llegar a su destino.

Los ruteadores son dispositivos que trabajan en esta capa (un término común que los ruteadores reciben es el de dispositivos de capa tres) y proporcionan los servicios de ruteo en una red.

Antes de enviar un paquete por la red, la computadora origen determina si el destinatario del paquete se encuentra en la misma red local o se encuentra en una red remota. Esto lo hace comparando la dirección lógica propia con la de destino. En caso de que el dispositivo destino se encuentre en la red local del dispositivo origen, el paquete se le envía directamente, en caso de que el paquete sea para un *host* remoto éste se envía al ruteador que conecta la LAN local a otras redes. Una vez que el paquete llega al ruteador, éste determina si el destino se encuentra en alguna de las redes que tiene directamente conectadas, en cuyo caso lo transmite directamente a la red o si el destino se encuentra en alguna de las redes remotas a él y, entonces lo remite al siguiente ruteador en la dirección hacia la red remota de destino. Este proceso sigue a través de los ruteadores necesarios hasta alcanzar el destino.

Existen dos tipos de paquetes que funcionan en la capa tres: los paquetes de datos y los paquetes de actualización de ruteo.

Los paquetes de datos llevan, precisamente, los datos que el usuario desea transmitir y para hacerlo deben utilizar algún protocolo que los ruteadores entiendan (los ruteadores no aceptan cualquier protocolo de comunicación.) Los protocolos capaces de llevar tráfico a través de ruteadores son protocolos ruteables y entre ellos se encuentran IP, IPX y Apple Talk.

Los paquetes de actualización de ruteo son los paquetes que los mismos ruteadores envían para conocer las redes que manejan otros ruteadores, el estado de éstos y las mejores rutas entre dos puntos considerando diferentes parámetros. Este tipo de paquetes utilizan protocolos de ruteo como son RIP, IPX RIP, IGRP, EIGRP y OSPF.

Algunos puntos importantes que recordar como parte de los conocimientos básicos en el campo de las redes y por ende importantes para el examen de Cisco son:

- Los ruteadores, por configuración predeterminada, no reenvían paquetes en *broadcast* ni en *multicast.*

- Los dispositivos en capa tres utilizan la dirección lógica en el encabezado correspondiente para determinar el siguiente salto (a cada ruteador en el camino que debe tomar un paquete hasta su destino se le llama "salto".)

- Los ruteadores pueden utilizar listas de acceso para controlar la seguridad en cuanto a los tipos de paquetes a los que se les permite el paso por alguna interfase.

2.5.6 Capa 2- Enlace de Datos

Esta capa recibe los paquetes de la capa inmediata superior y los descompone en *bytes* y a su vez combina los *bytes* para formar *Frames.* Es en esta capa en donde los

Frames reciben la dirección física del dispositivo de destino es decir el MAC de destino. Aquí se realiza la detección de errores al transmitir los *Frames* por la red.
La capa de enlace de datos se divide en dos sub-capas: LLC y MAC. Puede notarse que LLC es el estándar 802.2 y que al utilizarse en esta capa añade funcionalidad al establecer circuitos de comunicación. La sub-capa MAC, por otro lado integra al paquete la dirección física del dispositivo destino.

Los *switches* son dispositivos que normalmente trabajan en esta capa y utilizan el MAC para direccionar otros dispositivos. Los ruteadores, que trabajan en la capa tres, de hecho no ven dispositivos en particular sino redes enteras. Esto provee un esquema jerárquico de direccionamiento, lo que es mucho más funcional que tratar de ver todos los dispositivos en un mismo nivel. Cuando el ruteador entrega un paquete a una red en particular, es misión de los dispositivos de capa dos enviar dicho paquete a su destinatario particular y esto se logra a través de la dirección física de la tarjeta que el dispositivo tiene. A pesar de que cada paquete tiene grabada la dirección lógica de la máquina a la que debe llegar, a un nivel local es necesario encontrar los dispositivos por su dirección física.

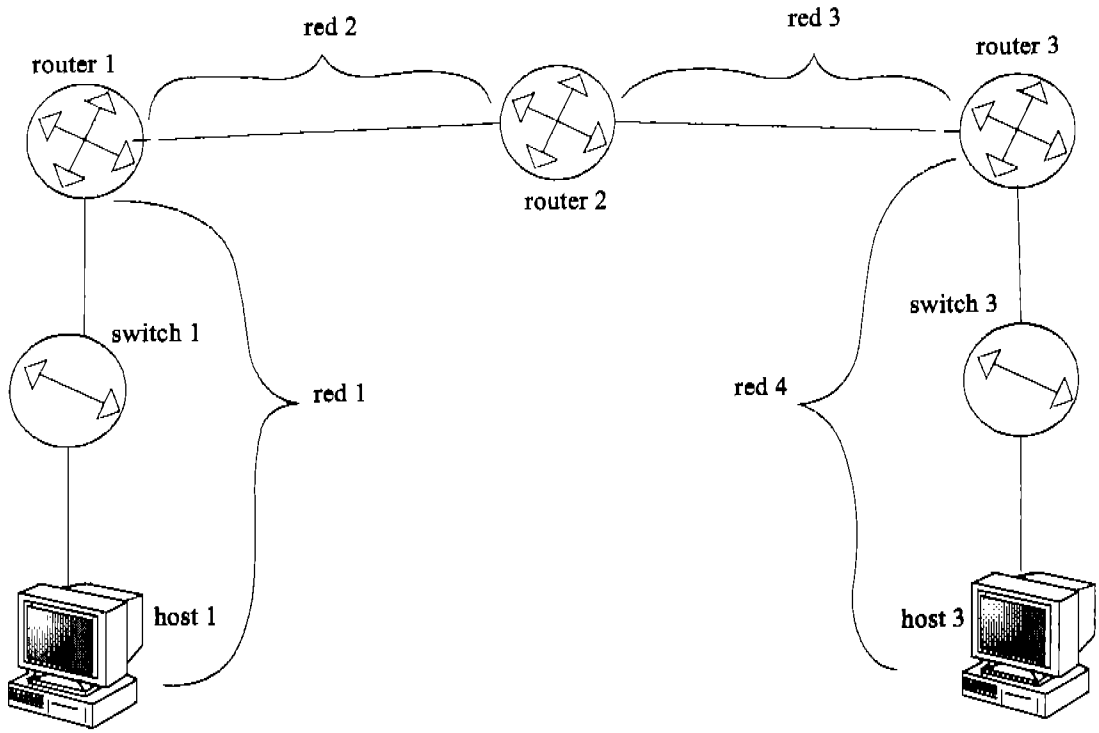


Figura 2.6 Envío de un paquete por medio de direccionamiento de capa dos y capa tres.

Véase el ejemplo en la figura 2.6. Supóngase que en esta red se utiliza TCP/IP y que el *host* 1 manda un paquete al *host* 2, los pasos que se seguirían para lograr el direccionamiento y por consiguiente la entrega de este paquete son los siguientes:

1. El *host* 1 determina, por medio de las direcciones lógicas, si el destinatario del paquete se encuentra en la misma red que él o si es remoto. En este caso el destinatario es un *host* remoto, por lo tanto, al paquete se le anexa la dirección lógica del *host* remoto en este caso el IP del *host* remoto pero también se le anexa la dirección física (el MAC) de la interfase del ruteador que pertenece a la red 1. El paquete se envía por medio del *switch* 1.

2. El *switch* 1 recibe el paquete y lee en el encabezado de éste la dirección física a la que va dirigido y lo envía por el puerto que está conectado hacia esa dirección.

3. El ruteador 1 recibe el paquete y lee el IP de destino. Después de leerlo, determina si la red a la que pertenece el paquete (en este caso la red 3) esta localmente conectada al ruteador. Como no lo está en este caso, busca en su tabla de ruteo cuál es el siguiente salto para llegar a la red 3 y cambia el MAC de destino en el paquete por el del siguiente ruteador, el ruteador 2.

4. El ruteador 2 recibe el paquete, lee el IP y determina si la red 3 está directamente conectada a él. Al ver que no, busca el siguiente salto y cambia la MAC de destino en el paquete por la MAC del siguiente ruteador en el camino hacia la red 3. El IP no ha sido modificado.

5. El ruteador 3 recibe el paquete, lee el IP y ve que la red 3 esta directamente conectada a una de sus interfases por lo que pone la MAC del *host* de destino en el paquete y lo envía por la interfase apropiada.

6. El *switch* 3 recibe el paquete, lee la MAC de destino y lo envía por el puerto que esta conectado a esta MAC.

7. El *host* 3 recibe el paquete y lo acepta después de realizar las comprobaciones de MAC, de IP y de que no hubo errores en la transmisión.

2.5.7 Capa 1-Física

La capa física se encarga de convertir los *Frames* que recibe de la capa enlace de datos en *bit*s y estos *bit*s en señales que viajen por el medio físico. En esta capa se especifican los parámetros físicos que se requieren para activar, mantener y desactivar la conexión entre dos dispositivos. Estos son parámetros eléctricos, mecánicos, de procedimientos y funcionales.

Viéndolo de manera muy simplista, la capa física hace dos cosas: enviar *bit*s y recibir *bit*s. Por supuesto que los *bit*s no pueden viajar como tales por medios físicos, por eso es necesario que antes de enviarlos, la capa física convierta los *bit*s a señales enviables por el medio que se esté utilizando y a la inversa, que las señales que reciba las convierta en *bit*s que son manejables por la computadora que recibe el

paquete. Los elementos que trabajan en esta capa son los repetidores, los *hubs* (que funcionan como repetidores de muchos puertos), los cables y, parcialmente, las tarjetas de red.

2.6 Modelo de Referencia DoD

El TCP/IP (*Transmission Control Protocol/Internet Protocol*) fue creado por el departamento de defensa de los Estados Unidos para asegurar y mantener comunicaciones en el caso de que estallara una guerra de proporciones catastróficas. De allí, que al configurarse correctamente, TCP/IP es un protocolo sumamente confiable.

El modelo DoD (*Department of Defense*) es el modelo creado como una versión condensada del modelo OSI para el conjunto de protocolos que integran el TCP/IP. En otras palabras, el modelo de referencia DoD es un modelo que solamente se utiliza para TCP/IP. El modelo DoD se compone de cuatro capas en lugar de las siete del modelo OSI:

- Capa Process/Aplication
- Capa *Host* to *Host*
- Capa Internet
- Capa *Network Access*

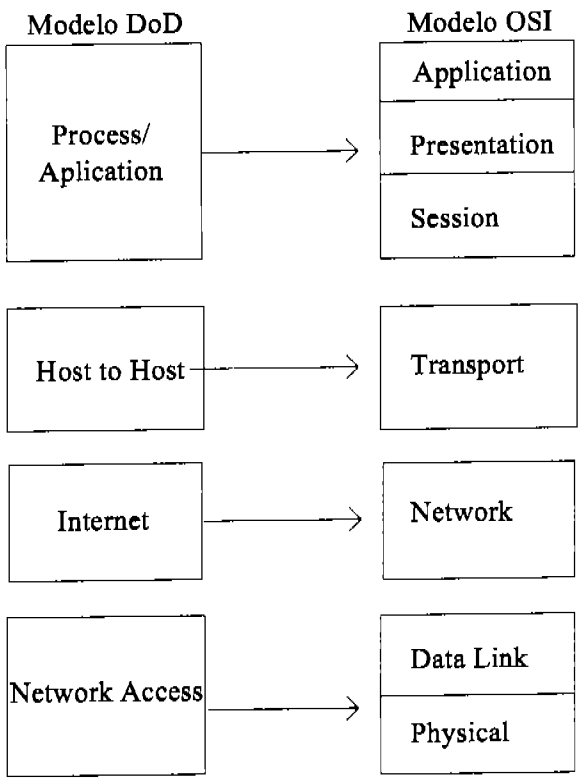


Figura 2.7 Comparación entre las capas del modelo OSI y las del modelo DoD

En la figura 2.7 se muestra una comparación de la equivalencia de las capas del modelo OSI contra las del modelo DoD.

La figura 2.8 muestra las diferentes capas del modelo DoD y los elementos más importantes que las conforman.

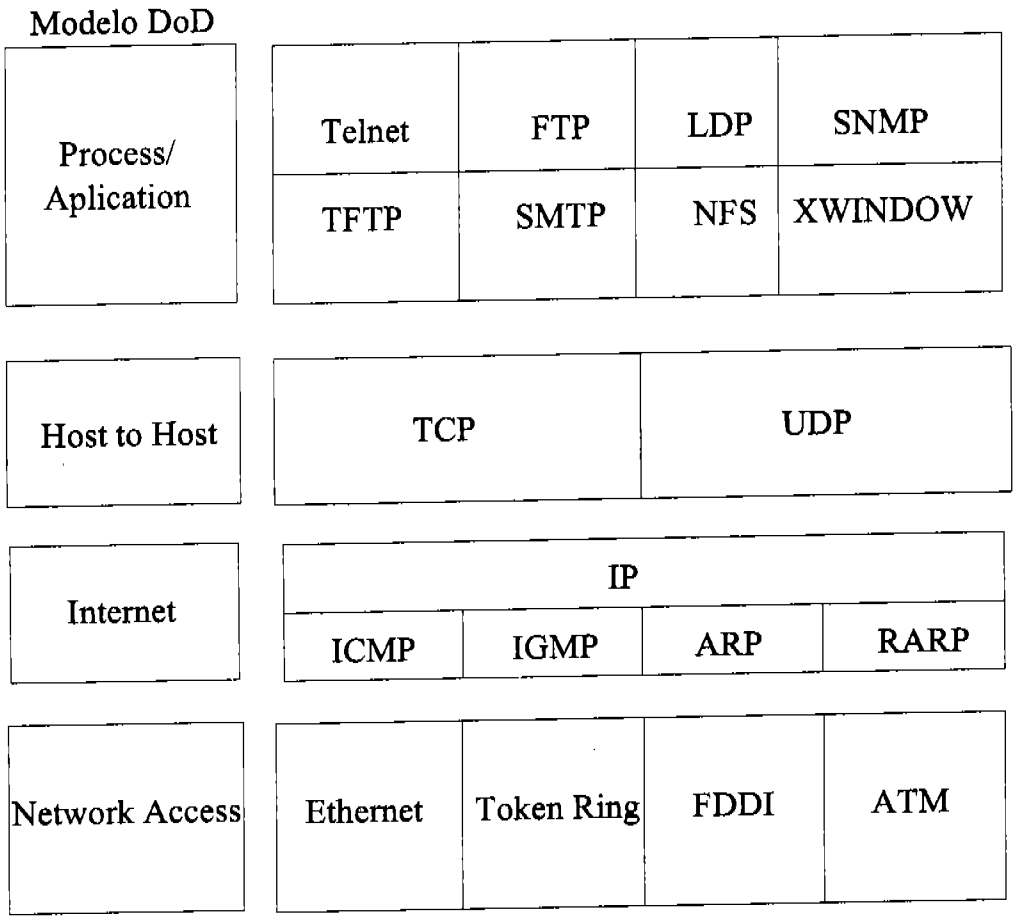


Figura 2.8 Conformación del modelo DoD

2.7 Protocolos de la Capa de Procesos y Aplicaciones

Hay una gran cantidad de protocolos que integran la capa de procesos y aplicaciones del modelo DoD y que en el modelo OSI corresponden a las tres capas superiores. En la capa de procesos y aplicaciones se definen los protocolos que permiten la comunicación de punto a punto de las aplicaciones. Además, en esta capa se controlan las especificaciones de interfase con el usuario.

Algunos de los servicios y protocolos más comúnmente utilizados de esta capa incluyen los siguientes:

- Telnet
- FTP
- NFS
- SNMP
- LPD
- NAT
- ICS
- X *Window*
- SMTP
- WINS
- DNS
- DHCP

Dado que estos servicios y protocolos no son específicamente parte del examen, se mencionan sólo de manera somera.

2.7.1 Telnet

Telnet es un emulador de terminales remotas que permite a un usuario tener acceso a un dispositivo remoto a través de línea de comandos. El dispositivo remoto se configura como el servidor de Telnet mientras que la terminal por la que se le accesa es el cliente Telnet. Telnet hace que el servidor pueda ser manejado por medio del cliente a través de línea de comandos, emulando sobre el cliente que se está frente al servidor. El nombre Telnet es contracción de la frase "*Telephone Network*", que es la manera en que la mayoría de las conexiones de acceso remoto ocurrían al momento de su implementación.

Algunas modificaciones a Telnet son:

Telnet por SSH (*Secure Shell*) que se utiliza para proveer sesiones seguras hacia Unix y Linux.

ICA (*Independant Computing Architecture.*) Citrix toma el principio de sesión remota de Telnet y le añade lo que llamó *metaframe* con lo que proporciona una emulación en ambiente grafico del servidor remoto.

Terminal Service es la versión modificada y actualizada de Microsoft para ICA (de hecho Microsoft compro la fuente a Citrix.)

2.7.2 *File Transfer Protocol* (FTP)

File Transfer Protocol (FTP) es un protocolo que nos permite transferir archivos entre computadoras a través de la red. FTP es comúnmente utilizado por varias aplicaciones y su uso es transparente al usuario. Sin embargo, es posible utilizarlo de

manera manual ya que además de ser un protocolo, FTP es un programa. Al utilizar FTP de manera manual, se tiene la capacidad de realizar algunas funciones con directorios y archivos tales como enlistarlos o moverlos. Normalmente, Telnet se une a FTP para proveer acceso transparente al servidor FTP y manejar los archivos. Es imposible ejecutar procesos de manera remota a través de FTP.

Para darse de alta a una máquina remota por medio de FTP, es necesario que el usuario se autentifique por medio de una clave y contraseña.

2.7.3 *Trivial File Transfer Protocol* (TFTP)

TFTP es la versión corta de FTP. TFTP no provee ninguno de los servicios de manejo o exploración de directorios ni de autentificación. Sin embargo, si se conoce exactamente la ruta en donde se encuentra el archivo a transferir, TFTP es una muy buena opción, ya que es rápido y fácil de usar. La única función de TFTP es transferir archivos y aunque no presenta características de control de errores o de seguridad para el usuario, los paquetes que envía son mucho más pequeños que los que envía FTP.

2.7.4 *Network File System* (NFS)

NFS es un protocolo que se especializa en permitir que dos sistemas de archivos que normalmente son incompatibles puedan transferir archivos entre ellos. El *software* para servidor de NFS permite que una porción de la RAM del servidor se utilice para almacenar archivos que pueden ser utilizados por clientes con diferentes sistemas operativos y, por supuesto con diferentes sistemas de archivos. De manera que, por ejemplo un servidor con Windows puede proveer servicio de transferencia de archivos a un cliente Unix, a pesar de que el sistema de archivos de Unix es diferente al NT de Windows. Además el cliente Unix realiza la función en un ambiente totalmente normal para Unix.

2.7.5 *Simple Mail Transfer Protocol* (SMTP)

SMTP se utiliza para mandar correo electrónico a través del método de colas. Cuando se envía un mensaje por correo electrónico, éste se almacena en un dispositivo el cual es revisado constantemente por el *software* del servidor que da servicio al destino, cuando se encuentran mensajes se procede a entregarlos a su destino. Mientras que SMTP se utiliza para mandar correo, POP3 (*Post Office Protocol versión* 3) e IMAP (*Internet Message Access Protocol*) se utilizan para recibirlo.

2.7.6 *Line Printer Daemon* (LPD)

LPD es un protocolo diseñado para compartir impresoras. LPD se utiliza en conjunto con LPR (*Line Printer*) para imprimir por medio de la red utilizando TCP/IP como

protocolo al enviar los documentos a imprimir. En otras palabras, a través de LPD y LPR es posible imprimir de manera remota, incluso entre sistemas operativos disimilares y aún desde locaciones en diferentes países a través de Internet.

2.7.7 *Network Address Translator* (NAT)

El *Network Address Translator* permite que varias computadoras compartan una o varias IP's públicas (por supuesto un número menor de IP's públicas que de computadoras que las comparten.) La manera en que el NAT comparte las IP's públicas que tiene es cambiando la dirección IP de origen de los paquetes de las computadoras a las que les da servicio por uno de los IP's públicos que tiene y reenviando estos paquetes hacia Internet. Al mismo tiempo que el paquete de una computadora con IP privado puede salir a Internet, la computadora origen está segura contra ataques por Internet ya que su IP real no es público.

2.7.8 *Internet Connection Sharing* (ICS)

Aunque muchas veces ICS se nombra por separado, éste es la versión casera de NAT en sistemas operativos de Microsoft. En específico, Windows ME, Windows XP, y la familia de Windows 2000 incluyen ICS en sus componentes. ICS permite compartir los servicios de Internet con una muy pequeña red de computadoras de manera fácil y muy directa, tal vez en esta misma sencillez de implementación radica su desventaja ya que no provee gran seguridad a los usuarios.

2.7.9 X *Window*

X *Window* fue diseñado para escribir aplicaciones basadas en GUI (*Graphic User Interface*) para operaciones cliente / servidor. La idea general es permitir que un programa, llamado cliente X *Window*, se ejecute en una computadora y haga desplegados por medio del servidor en otra computadora.

2.7.10 *Simple Network Management Protocol* (SNMP)

SNMP es un protocolo para monitoreo de la red. En términos llanos, SNMP permite tomar un muestreo de estado a todos los dispositivos en la red. Este muestreo se almacena en un sistema central. SNMP también permite establecer parámetros hacia cualquier dispositivo de la red desde el sistema central de monitoreo.

El sistema central de monitoreo, conocido como manager tiene en su historial una línea de base del comportamiento de la red en circunstancias normales y el administrador de la red define las diferencias máximas admisibles en varios puntos de interés del monitoreo. Cada dispositivo en la red que se maneja por medio de este protocolo está corriendo un *software* conocido como el agente SNMP que comunica la ocurrencia de ciertos eventos, fuera de los parámetros definidos por el

administrador de la red, conforme suceden al sistema manager. Estos avisos se conocen como trampas.

Una herramienta muy útil al emplear SNMP es NMS (*Network Management System*) que permite realizar las funciones de muestreo y configuración (conocidas como el paradigma *get/set*) de manera gráfica. NMS permite navegar por un mapa de la red y por medio del mouse obtener información o incluso establecer parámetros a cualquiera de los dispositivos que estén corriendo en ellos el agente SNMP.

2.7.11 *Windows Internet Name Service* (WINS)

En plataformas Windows, WINS permite resolver los nombres tipo NetBIOS a direcciones IP. Por supuesto que es mucho más fácil para una persona el recordar un nombre de computadora como servidor2, que un IP como 172.16.23.165.

Existen tres formas en las que se resuelve un nombre NetBIOS a su dirección IP:

1. La más sencilla es utilizando un servidor WINS que automáticamente realiza el trabajo.
2. La segunda forma, y normalmente utilizada cuando no se tiene disponible el servidor WINS es a través de un archivo estático en el que el administrador configura manualmente una tabla de mapeo de nombres NetBIOS contra sus respectivos IP's. Las desventajas de utilizar este archivo llamado LMHOSTS son el tiempo requerido para configurarlo y actualizarlo y, que no se mantiene automáticamente con los cambios que ocurren en la red, además, al ser configurado manualmente, es más susceptible de errores que utilizando WINS.
3. La tercera forma de resolver a una dirección IP teniendo un nombre NetBIOS es a través de *broadcasts*. Y aunque esta es la forma habilitada de manera predefinida en la mayoría de los sistemas operativos, tiene dos desventajas muy importantes: la primera es el tráfico que provoca en la red y la segunda es que los ruteadores no retransmiten *broadcasts* por lo que este método solo resuelve nombres de máquinas en el mismo segmento.

2.7.12 *Domain Name Service* (DNS)

DNS realiza una función análoga a WINS pero con nombres de máquina del tipo *hostnames*. Los nombres *hostnames* son independientes a la plataforma por lo que DNS puede resolver *hostnames* a IP's para sistemas Windows, Linux, Unix, NetWare y prácticamente cualquier otra plataforma. DNS es un protocolo independiente a la plataforma. Al igual que con WINS, los *hostnames* se pueden resolver de tres maneras:

1. Por medio de servidor DNS.
2. Por medio de un archivo estático, en este caso llamado *Hosts file*.
3. Por medio de *broadcasts*.

En específico, los *hostnames* son los nombres utilizados en Internet, que normalmente se escriben en su forma de FQDN (*Fully Qualified Domain Name*) como www.raul.martinez.com.

DNS utiliza el algoritmo de *forward lookup query* para resolver los *hostnames* a sus respectivos IP's y el algoritmo *backward lookup query* para resolver IP's a sus respectivos *hostnames*.

2.7.13 *Dynamic Host Configuration Protocol* (DHCP)

DHCP es un protocolo muy útil, en especial en redes grandes ya que se encarga de asignar IP's y algunos otros parámetros como máscara de sub-red, nombre de dominio, puerta de salida, DNS, WINS.

Al iniciar un *host* configurado para obtener su información TCP/IP de manera dinámica, éste busca el servidor DHCP a través de un *broadcast* en que informa su necesidad de una IP. El DHCP responde al *broadcast* con un *unicast*, dirigido al *host* en particular, en el cual le propone un IP disponible dentro del rango que el DHCP maneja. El *host* acepta el IP y envía un *unicast* al servidor DHCP en el que le comunica que ha aceptado los nuevos parámetros propuestos. El DHCP retira el IP asignado de su tabla de IP's disponibles y envía un mensaje más al *host* para confirmar que ha tomado la dirección IP que le asignó. (Aunque parece que el proceso de asignación es muy redundante, éstos son los pasos oficialmente aceptados por Microsoft)

Cabe mencionar algunos detalles importantes en cuanto a la implementación de DHCP:

El *host* que requiere una IP no tiene una IP. Lo anterior es obvio pero la implicación no lo es tanto: al no tener IP, el *host* no puede utilizar TCP/IP para transmitir. Por lo tanto, el paquete que el *host* transmite no es ruteable. En otras palabras, el cliente de DHCP tiene que estar en el mismo segmento de red que el servidor.

En algunos sistemas operativos, si el cliente no recibe respuesta del servidor DHCP, entonces entra en APIPA (*Automatic Private IP Addressing*) que es un proceso por el cual el *host* se asigna a sí mismo una dirección IP en el rango de 169.254.0.1 hasta 169.254.255.254.

Para que un *host* pueda accesar a un servidor DHCP en otra sub-red es posible establecer un agente de relevo el cual es una computadora en el mismo segmento que entiende el *broadcast* de búsqueda de DHCP y finge ser el servidor DHCP hacia el *host* pero a su vez, fingiendo ser el *host* que necesita un IP, envía los mismos paquetes en TCP/IP a través de un ruteador y con la dirección específica del servidor DHCP en otro segmento.

Actualmente, muchos ruteadores realizan ellos mismos la función de un agente de relevo, por lo que entienden y reenvían los paquetes de *broadcast* en busca del servidor DHCP. Estos ruteadores se conocen como 1542-compliant ya que cumplen con las características definidas en RFC[4] 1542.

Una versión temprana de DHCP es BOOTP (*Bootstrap Protocol*) y tiene en esencia la misma funcionalidad del DHCP normal, con la diferencia de que el BOOTP se creó originalmente para permitir a terminales tontas, computadoras sin disco, obtener la información TCP/IP necesaria para conectarse a la red y de allí recibir un sistema operativo. Una de las principales desventajas de BOOTP ante DHCP es que la dirección física del *host* debe ser introducida manualmente en la tabla de BOOTP.

2.8 Protocolos de la Capa *Host to Host*

En la capa *Host* to *Host* solamente existen dos protocolos TCP y UDP.

Esta capa se encarga de las transmisiones por la red como un servicio a la capa superior, de modo que la capa de Procesos y Aplicaciones sea independiente de los envíos de sus propios paquetes.

2.8.1 *Transmission Control Protocol* (TCP)

TCP es un protocolo orientado a la conexión y confiable, es decir que antes de enviar cualquier paquete de información por la red, TCP establece una conexión o un circuito virtual determinando el camino que los paquetes seguirán durante la comunicación. Además, cada paquete que se envía por TCP se reconoce por el sistema de destino con un mensaje de *Acknowledgment* positivo.

TCP toma el archivo a enviar de la capa de Procesos y Aplicaciones y lo segmenta en pequeños trozos de información. A estos trozos se les llaman segmentos. Cada segmento se enumera a modo que el TCP en el extremo receptor los pueda reacomodar en el orden correcto antes de entregarlos a su capa superior.

Cada aplicación en la capa superior genera un identificador propio que pasa a la capa de transporte o *host* to *host* y con el cual TCP o UDP saben a qué aplicación pertenecen los segmentos recibidos. A este identificador se le llama puerto.

Para establecer la conexión TCP utiliza el algoritmo conocido como *Three Way Handshake* (la traducción literal sería: Apretón de manos de tres vías.) En mis cursos de preparación para la certificación, me gusta referirme al *Three Way Handshake* como el "-¿Quihubo?... –¡Quihubo! ...-¿Cuándo?" (Saludo clásico de Pedro Infante y Jorge Negrete en sus películas.) Véase la figura 2.9

[4] RFC (Request For Comments) es una serie de notas técnicas iniciadas en 1969 que discuten varios aspectos de computadoras y comunicaciones.

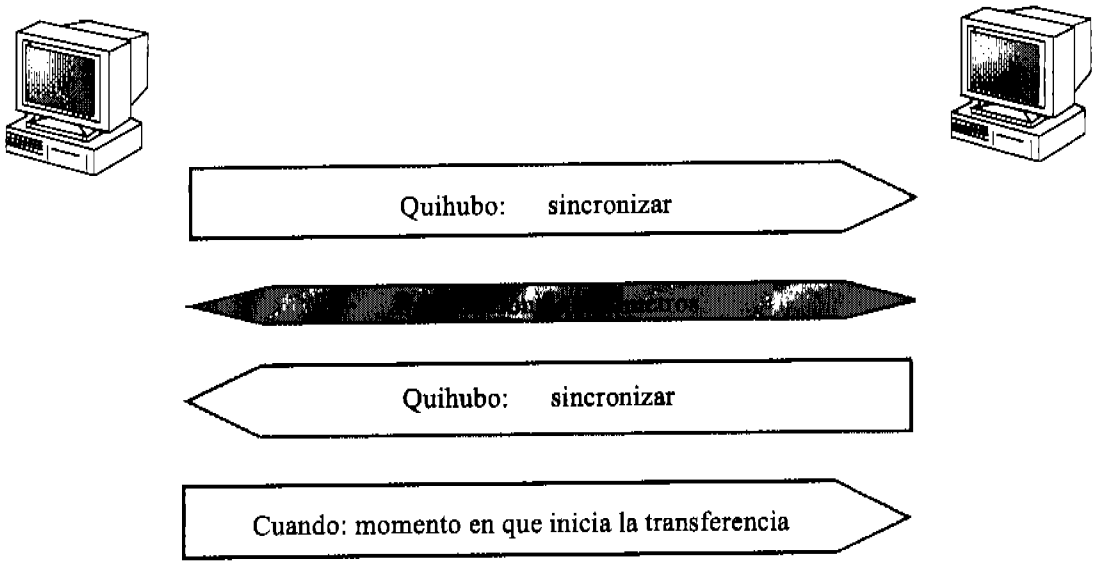


Figura 2.9 Three Way Handshake.

En la figura 2.9 se ilustran los tres pasos al establecer una transferencia orientada a la conexión:

- En el primer quihubo, como sucedía en las películas, el emisor se anuncia. En el caso de las computadoras, en ese mensaje se anuncia la intención de transmitir, y los datos particulares del emisor, además de los parámetros que se proponen para la transmisión como son la velocidad, el tamaño de la ventana, etc. después de este primer mensaje de sincronía se negocian dichos parámetros.
- El quihubo de respuesta es igual al primero emitido, es decir, a través de este mensaje, el receptor envía sus datos particulares.
- El cuándo indica, precisamente, cuando se comienza con la transferencia de segmentos: a partir de que se recibe este mensaje.

Periódicamente, después de establecerse la conexión, ésta se revisa para asegurarse de que la transmisión se está efectuando correctamente.

Según el tamaño de la ventana que se esté utilizando, el emisor envía ese número de octetos y espera recibir un *Acknowledgment*[5].

Después de que TCP rompe la información que recibe desde la capa superior en segmentos, a cada segmento le añade un encabezado que incluye la información necesaria para manejar el segmento en la capa de Internet hacia abajo y la capa de Procesos y Aplicaciones hacia arriba. Esta información se muestra en la figura 2.10 que contiene el formato de un segmento TCP.

[5] Véanse las figuras 2.4 en la página 57 y 2.5 en la página 58

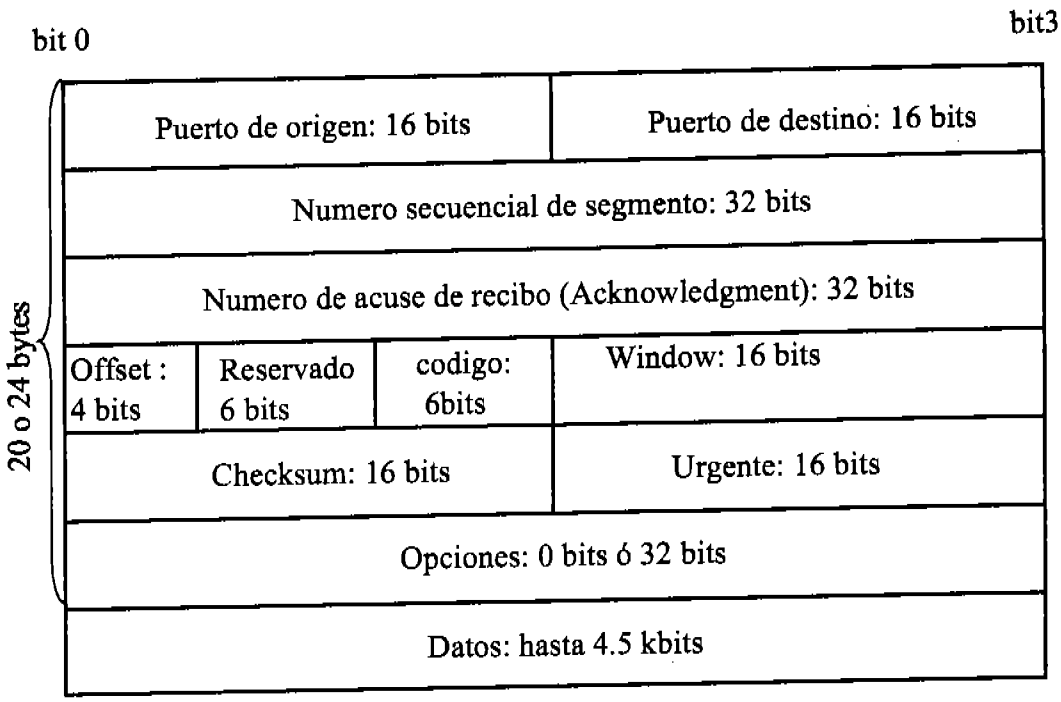


Figura 2.10 Formato de un segmento TCP.

El encabezado de TCP tiene una longitud de 20 (si se utilizan opciones 24) *bytes* e incluye los siguientes campos:

- Puerto de origen.- Un número calculado de acuerdo a la instancia en particular que se está corriendo.
- Puerto de destino.- El puerto que identifica la aplicación específica a la que va dirigido el segmento. Si esta aplicación es una aplicación común, generalmente tiene un puerto bien conocido que se reconoce por estar en el rango de 0 a 1023. Otras aplicaciones e instancias utilizan los puertos 1024 a 65535.
- Número secuencial de segmento.- Este número se utiliza para identificar los segmentos que pudieran llegar dañados y solicitar una retransmisión de éstos y para ordenar los segmentos antes de pasar la información a la capa superior.
- Número de *Acknowledgment*.- Con este número se pide el siguiente octeto a recibir.
- *Offset*.- El *offset* indica qué parte del segmento es encabezado y donde comienzan los datos.
- Reservado.- Siempre lleva 6 *bits* en cero.
- Código.- Tiene un número que controla el inicio el manejo y la terminación de la sesión.
- *Window*.- Especifica el número de octetos que el emisor está dispuesto a aceptar en una sola ventana.

- *Checksum*.- En este campo se incluye el resultado del CRC (*Cyclic Redundancy Check*) que es un algoritmo que cuenta el número de unos en el envío. Al recibir el segmento se vuelve a calcular ese número y se compara con el que se encuentra en el campo. Si el número calculado y el enviado no son iguales, seguramente el segmento ha sufrido cambios en el camino y habrá que retransmitirlo. En los segmentos el *checksum* se aplica al encabezado y a los datos.
- Urgente.- Solamente se utiliza si se ha definido en los *bit*s de código, e indica en que octeto comienza la información no urgente.
- Datos.- La información segmentada de la capa superior por TCP.

2.8.2 *User Datagram Protocol* (UDP)

UDP es mucho más ligero que TCP ya que no realiza funciones de revisión de errores o retransmisión de segmentos. Al enviar un segmento, UDP lo hace bajo el mejor esfuerzo, es decir, lo envía lo mejor que puede pero después de enviado no le interesa si el segmento llegó bien al destino. UDP tampoco se interesa en que los segmentos puedan ser reordenados en el extremo receptor, ni siquiera acepta que se le envíe algún tipo de *Acknowledgment*. A diferencia de TCP, UDP es un protocolo no confiable. Esto no significa que UDP sea ineficiente, sino únicamente que no realiza funciones de confiabilidad de entrega.

Al enviar sus segmentos, UDP no necesita establecer un circuito virtual, o conexión, antes de iniciar la transferencia. Los segmentos de UDP, como dijera Joan Manuel Serrat, hacen camino al andar. Por esto, UDP además de ser no confiable es no orientado a la conexión.

Las ventajas principales de un protocolo tan poco interesado en la seguridad de entrega, son transmisiones más rápidas y menor consumo de ancho de banda. Estas características lo hacen el protocolo ideal para enviar *broadcasts*. Sería demasiado desperdicio enviar un *broadcast* y esperar un *Acknowledgment* de cada computadora en el segmento de red y aún más desperdicio el retransmitir un *unicast* hacia cada una de las computadoras que no recibieron el *broadcast*. ¡Esto no se hace!

Las transmisiones UDP se utilizan principalmente en aplicaciones de transferencia rápida de datos como TFTP, en aplicaciones de videoconferencia o audio en tiempo real, y en general en aplicaciones en las que la aplicación misma se encarga de la confiabilidad de la transmisión.

La figura 2.11 muestra un segmento UDP. En ella se nota claramente cómo este tipo de segmentos tiene una carga muy inferior a la que tiene TCP. Nótese que UDP no tiene un campo para definir el *Windowing* o siquiera un campo de *Acknowledgment*.

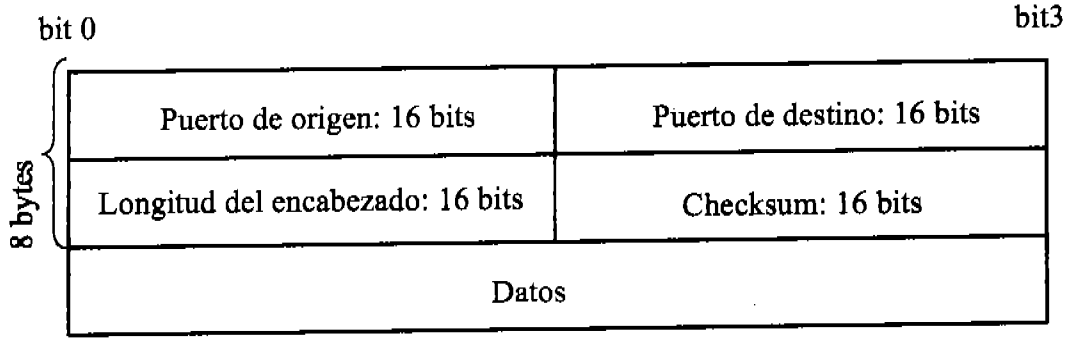


Figura 2.11 Formato de un segmento UDP.

UDP se discute ampliamente en el RFC 768.

2.8.3 Puertos

Tanto UDP como TCP reciben de la capa de aplicaciones y procesos un número que identifica la instancia del proceso que está mandando la información. Este número se utiliza por la capa de transporte o *host* to *host* para dirigir los segmentos recibidos a la aplicación correcta.

Los puertos se clasifican en los "Bien conocidos" que son los puertos menores a 1024 y se definen en el RFC 3232. Véase la figura 2.12

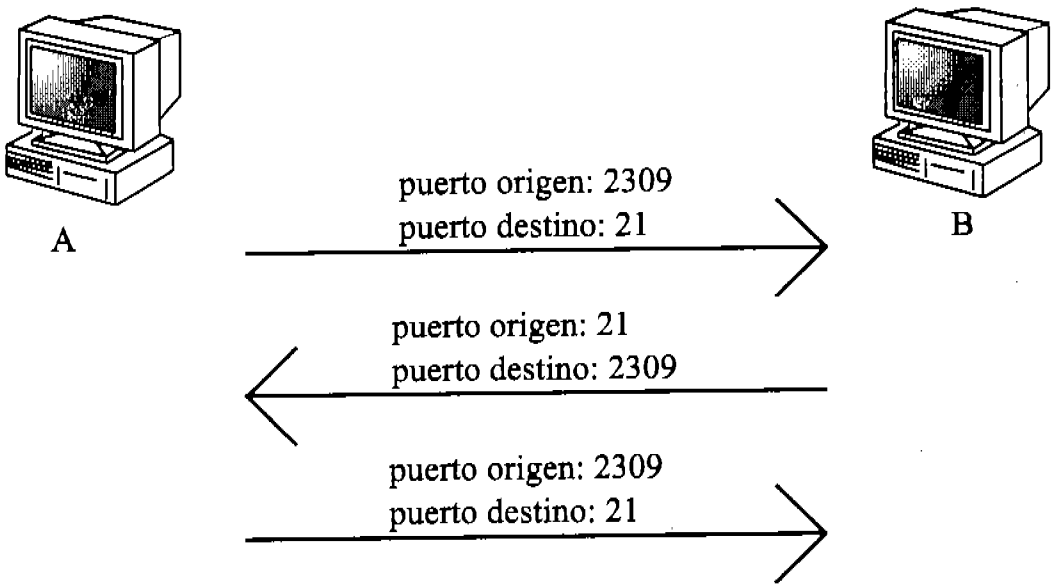


Figura 2.12 Ejemplo de utilización de puertos.

En el ejemplo de la figura 2.12 :

- El primer segmento que se envía de la computadora A a la B lleva un puerto de origen calculado en particular para la instancia de la aplicación que se está utilizando, este puerto es mayor a 1023 (el rango numérico que los puertos pueden tomar es de 0 a 65535.) En este caso el puerto de origen es 2309. El puerto de destino en este ejemplo es 21, un puerto bien conocido que identifica que la aplicación a la cual va dirigido este segmento es FTP.

- Al llegar a su destino el primer segmento se dirige a la aplicación FTP. Si varios usuarios están transfiriendo archivos por FTP será fácil identificar la instancia que cada uno está utilizando, porque sus puertos de origen son diferentes para cada computadora e incluso si un mismo cliente está utilizando varias instancias de la misma aplicación cada una tendrá un diferente puerto de origen.

- Al responder, los puertos de origen y de destino se intercambian según el sentido en que viajan los segmentos. Y así sucesivamente.

Además de servir para comunicarse con la capa equivalente en otra computadora los puertos permiten a las capas adyacentes dirigir la información más eficazmente. La figura 2.13 muestra algunos de los puertos más utilizados entre las capas de *host* to *host* y de aplicaciones y procesos.

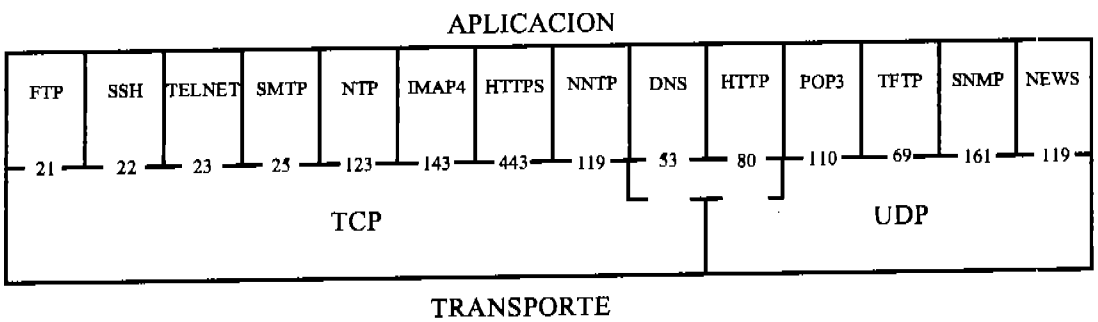


Figura 2.13 Principales puertos entre las capas de aplicación y de transporte.

2.9 Protocolos de la Capa de Internet.

La capa de Internet del modelo DoD tiene como principal función: proveer ruteo para los segmentos que recibe de las capas superiores. Ninguna de las otras capas en el modelo tiene alguna función de ruteo. Una vez más: ¡El ruteo pertenece única y exclusivamente a la capa de Internet!

Como complemento a su función principal, la capa de Internet tiene solamente otra función: ser la interfase entre la red y las capas superiores. De este modo las

aplicaciones no son dependientes del modo de transmisión como *Ethernet* o *Token Ring* y por lo tanto no es necesario que cada aplicación considere una versión para *Ethernet* y una más para ser transmitida en un *Token Ring*.

2.9.1 *Internet Protocol* (IP)

Todo paquete que para su transmisión utiliza TCP/IP, sin importar si es a través de TCP o UDP, o la aplicación, o la topología, o cualquier otra consideración, utiliza los servicios de IP. IP es un protocolo no orientado a la conexión y no confiable.

IP es el servicio que asigna direcciones lógicas a los dispositivos en la red. Más aun, IP tiene la facultad de ver todas las redes y sub-redes que intervienen en un entorno. La dirección lógica que IP asigna se conoce como IP y se compone de dos partes: la primera parte identifica la red a la que pertenece la dirección y por consiguiente el *host* que la posee y la segunda parte identifica en específico al dispositivo. De este modo el direccionamiento por IP es jerárquico, primero buscando la red entera y después el dispositivo en particular en dicha red.

IP decide, basándose en la red de origen y la red de destino de un paquete, si el destinatario es local o remoto al origen, es decir si están en la misma red o no. En caso de que el destino sea local, la computadora origen envía el paquete directamente al destino; pero si el destino es remoto, la computadora origen envía el paquete al *default gateway* (puerta de salida) que normalmente es un ruteador, el cual determina el siguiente salto en el camino hacia la red de destino.

Al igual que sucede entre las capas de aplicación y de transporte, la capa de Internet necesita de puertos para saber a qué protocolo enviar los paquetes que recibe pero a diferencia de los 65536 puertos disponibles entre aquellas capas, entre transporte e Internet hay pocas opciones y los números de puertos entre estas últimas son en hexadecimal. Véase la figura 2.14

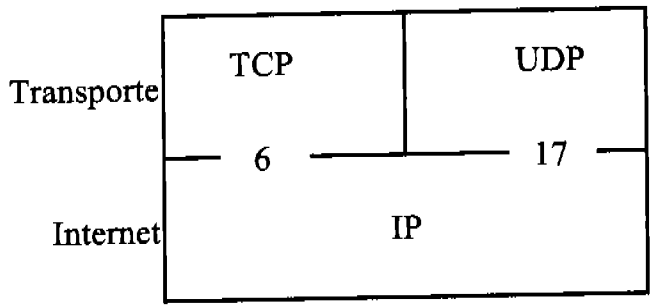


Figura 2.14 Puertos entre las capas de Transporte y de Internet [Hex]

IP recibe los segmentos que provienen de la capa de transporte y les añade un encabezado propio en el que se encuentran el IP de origen y el IP de destino entre otras cosas. A la unidad de datos resultante se le llama paquete.

La figura 2.15 muestra el encabezado IP.

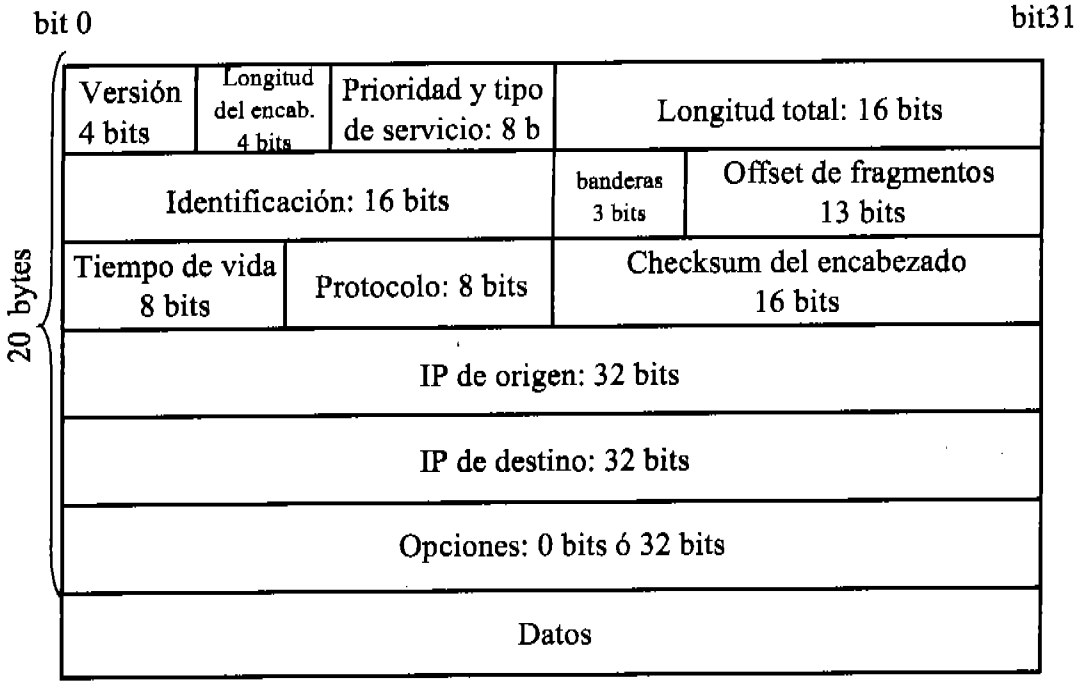


Figura 2.15 Encabezado IP.

Los campos de un paquete son los siguientes:

- Versión. Número de versión de IP.
- Longitud del encabezado. La longitud en palabras de 32 *bit*s que tiene el encabezado.
- Prioridad y tipo de servicio. Los tres primeros *bit*s determinan la prioridad del paquete. El tipo de servicio indica la función del paquete mismo.
- Longitud total. Longitud del paquete incluyendo el encabezado y los datos. (Recuérdese que los datos de este paquete se forman por el segmento de la capa superior)
- Identificación. En este campo aparece un identificador único del paquete.
- Banderas. Indican si se permite la fragmentación de los paquetes.
- Offset de fragmentación. Si el paquete es demasiado grande, este campo provee el tamaño máximo de los fragmentos que se pueden formar con él. Además de los indicadores necesarios para su reensamble en el extremo receptor. En Internet, este campo maneja el MTU (*Maximum Tansmission Units*) que determinan el tamaño máximo de fragmento que el emisor está dispuesto a aceptar.
- Tiempo de vida o TTL. El TTL es un número que se le agrega al paquete y se va decrementando con cada salto por un ruteador en la red. Cuando el TTL llega a cero, el paquete es destruido. Este procedimiento evita que los

paquetes perdidos, que no pueden encontrar la red de destino en el entorno, deambulen por la red indefinidamente, creando basura.

- Protocolo. En este campo se incluye el número de puerto (en hexadecimal) que identifica el protocolo al que se dirige el paquete. En el caso de que el paquete sea parte de un envío a las capas superiores, este campo sólo puede tener dos posibilidades: 6 ó 17 que identifican a los protocolos TCP y UDP respectivamente. Otra posibilidad es que el paquete sea de control y vaya dirigido a alguno de los protocolos de esta capa en cuyo caso identificará a ICMP, IGMP, IGRP, EIGRP, OSPF, IPv6, L2TP, etcétera. Véase la tabla 2.1
- *Checksum* del encabezado. El resultado del CRC aplicado solamente al encabezado. (A los datos ya se les aplicó en la capa superior)
- IP de origen. IP de la computadora que emite el paquete.
- IP de destino. IP de la computadora a la que se envía el paquete.
- Opciones. Se utilizan para pruebas de conectividad en de la red y seguridad.
- Datos. Incluyen los datos que recibió la capa de Transporte desde la capa de Aplicación más el encabezado de la capa de transporte. En otras palabras, contiene el segmento que se formó en la capa de Transporte.

IP se discute en RFC 791.

Protocolo	Número de protocolo [Hexadecimal]
ICMP	1
IGRP	9
EIGRP	88
OSPF	89
Ipv6	41
GRE	47
IPX en IP	111
L2TP	115

Tabla 2.1 Algunos protocolos de la capa de Internet.

2.9.2 *Internet Control Message Protocol* (ICMP)

ICMP es uno de los protocolos que dan soporte a IP y se utiliza para varios servicios. Una de las funciones principales de ICMP es, sin duda, la de monitor de la conectividad en la red. Dos de los comandos más conocidos relacionados con ICMP son *Ping* y *Traceroute*.

Ping (*Paket Internet Groper*) utiliza mensajes de ICMP llamados *echo request* y *echo reply* para determinar el estado de una conexión tanto física como lógica. El envío de los paquetes de eco se asemeja mucho, y probablemente de allí su nombre, a las emisiones sonoras que hace un radar de submarino llamadas eco. Al encontrar algún objeto en su camino, el eco rebota hacia el submarino y por medio de algunos cálculos es posible determinar varias características del objeto.

Ping utiliza un paquete de 32 *bytes* con el alfabeto en su campo de datos para comprobar la conectividad entre dos *hosts* (100 *bytes* por *default* para ruteadores Cisco.)

Traceroute o Trace se utiliza para determinar la ruta que sigue un paquete al viajar de un *host* a otro. Hay que tener cuidado de no confundir el comando Traceroute de Cisco con el Tracert de Microsoft. Los dispositivos Cisco no reconocen el comando Tracert.

2.9.3 *Address Resolution Protocol* (ARP)

La función de ARP es determinar el MAC correspondiente a cierto IP al enviar un paquete.

Cuando una máquina va a enviar un paquete a otra normalmente conoce el IP de destino. Sin embargo, al viajar en una red local, es necesario enviar los paquetes a la dirección física (MAC) del destinatario. La máquina de origen busca en su tabla ARP que guarda en RAM para determinar el MAC correspondiente a la IP que tiene. En caso de no encontrar en la tabla ARP una entrada que corresponda al IP dado, se manda un *broadcast* en el que se publica el IP para el que se busca la MAC correspondiente. La máquina cuyo IP coincide con el enviado, recibe el paquete y después de guardar en su propia tabla ARP el IP y MAC de la computadora que envió el *broadcast*, le contesta en un *unicast* diciendo su MAC. La máquina que inicialmente buscaba el MAC correspondiente al IP que tenía recibe el *unicast* e integra en su tabla la dirección física correspondiente al IP en cuestión. Después de esto manda el paquete con un *unicast* directamente a la IP de destino con el MAC correspondiente.

2.9.4 *Reverse Address Resolution Protocol* (RARP)

RARP se utiliza en el caso inverso que ARP. Es decir cuando se tiene un MAC para el cual se desea obtener el IP correspondiente.

Un caso en el que comúnmente se utiliza RARP, es al arrancar una computadora sin disco duro y por consiguiente sin sistema operativo ni IP. Al arrancar la computadora puede determinar su propio MAC pero no conoce su IP. En este caso la computadora utiliza RARP para obtener su IP del servidor RARP que lo contiene.

2.9.5 *Internet Group Management Protocol* (IGMP)

El IGMP provee a la capacidad de enviar paquetes en *multicasting*[6], es decir, a varias computadoras simultáneamente pero no a todas. Para lograr esto, IGMP

[6] Véase la figura 2.1

almacena listas de suscripción en las que define los grupos de computadoras que deben recibir los paquetes destinados a ciertos grupos.

2.10 Capa de *Network Access*

La capa de *Network Access* que es la más baja en el modelo DoD es equivalente a las capas Enlace de datos y física del modelo OSI. Esta capa recibe los paquetes que la capa superior quiere enviar por la red y los trata como datos en una nueva unidad de datos a la que le añade su propio encabezado y un campo al final llamado CRC que, en efecto, alberga el *Checksum* de todo el *Frame*, incluyendo los encabezados, los datos a los que ya se les hizo el *Checksum* en las capas superiores. A la unidad de datos en esta capa se le llama *Frame*.

El encabezado en esta capa incluye el MAC de origen y el MAC de destino y un preámbulo que consta de siete *bytes* que contienen el número AA en hexadecimal y un *byte* más que contiene el número AB entre otras cosas.

El preámbulo en binario es una sucesión de unos y ceros alternados y al final de ellos un par de unos. La intención de este preámbulo es suministrar una oscilación para que el sistema que recibirá el *Frame* pueda sincronizarse. El preámbulo proporciona un reloj a 5Mhz al inicio de cada *Frame*, el cual termina con un par de unos que determinan el inicio de la transferencia. De este modo aún si el receptor comenzó a recibir el *Frame* a la mitad del preámbulo, sabrá en que momento comienza la transmisión. Otra ventaja importante de utilizar un preámbulo es que generalmente hay inducciones electromagnéticas en los cables de red, estas inducciones pueden llegar a considerarse como un uno lógico seguido de muchos ceros lógicos, y pudiera generar basura que las tarjetas de red tratarían de entender.

El preámbulo evita que las tarjetas de red traten de entender cualquier combinación de ceros y unos que no sea precedida por la combinación del preámbulo específicamente, una combinación que es prácticamente imposible que se genere de manera aleatoria por EMI.

Al salir de la capa de *Network Access*, los *Frames* se convierten a *bits* y a señales eléctricas (lo que en el modelo OSI hace la capa física.)

2.11 Encapsulamiento

En cada una de las capas inferiores del modelo OSI se maneja una unidad de datos diferente debido a que se compone de diferentes elementos. Cuando una computadora transmite datos hacia otro dispositivo, estos datos pasan por cada una de las capas del modelo OSI, y en cada una de estas capas se les agrega información importante para la capa correspondiente en el extremo receptor. Cada capa considera como datos el PDU (*Protocol Data Unit*) recibido por la capa superior y agrega su propio encabezado. A esto se le llama encapsulamiento.

Con el encapsulamiento, cada capa tiene forma de comunicarse con las capas superior e inferior pero principalmente con la capa correspondiente en el sistema de destino. En el destino, cada capa lee la información preparada para sí y la elimina del PDU pasando hacia la capa superior solamente lo que considera datos pero que en realidad contiene el siguiente encabezado. A esto se le llama desencapsulamiento.

La figura 2.16 ilustra el encapsulamiento y desencapsulamiento.

El simple envío de información de una computadora a otra conlleva un sinnúmero de procesos y funciones. A grandes rasgos, lo que sucede en las capas inferiores cuando una computadora envía un archivo a otra por FTP es lo siguiente:

- El PDU en las capas superiores llamado datos se segmenta al ser recibido por la capa de transporte. Considérese que por tratarse de FTP, la transmisión se hará por TCP. Cada segmento se enumera y recibe un encabezado que entre otras cosas contiene el número de secuencia del segmento, los puertos de origen (por ejemplo 23400) y de destino (21), el tamaño de la ventana (3 para el ejemplo) y el CRC de todo el segmento. El PDU en la capa de transporte se llama segmento. En la capa de transporte se guarda una copia de los segmentos que se pasan a la siguiente capa.

- Al llegar a la capa de red, los segmentos se almacenan en al campo de datos en el nuevo PDU que se llama paquete. En el paquete que se forma, se incluye un encabezado que contiene entre otras cosas el IP de origen y el IP de destino, un CRC que se aplicó sólo al encabezado y el protocolo de esta capa al que va dirigido el paquete (TCP en este caso.) Como TCP es orientado a la conexión, comienza el algoritmo llamado *Three Way Handshake* para establecer la conexión antes de transmitir la información. En esta capa se determina si la computadora de destino se encuentra en la misma red que la de origen.

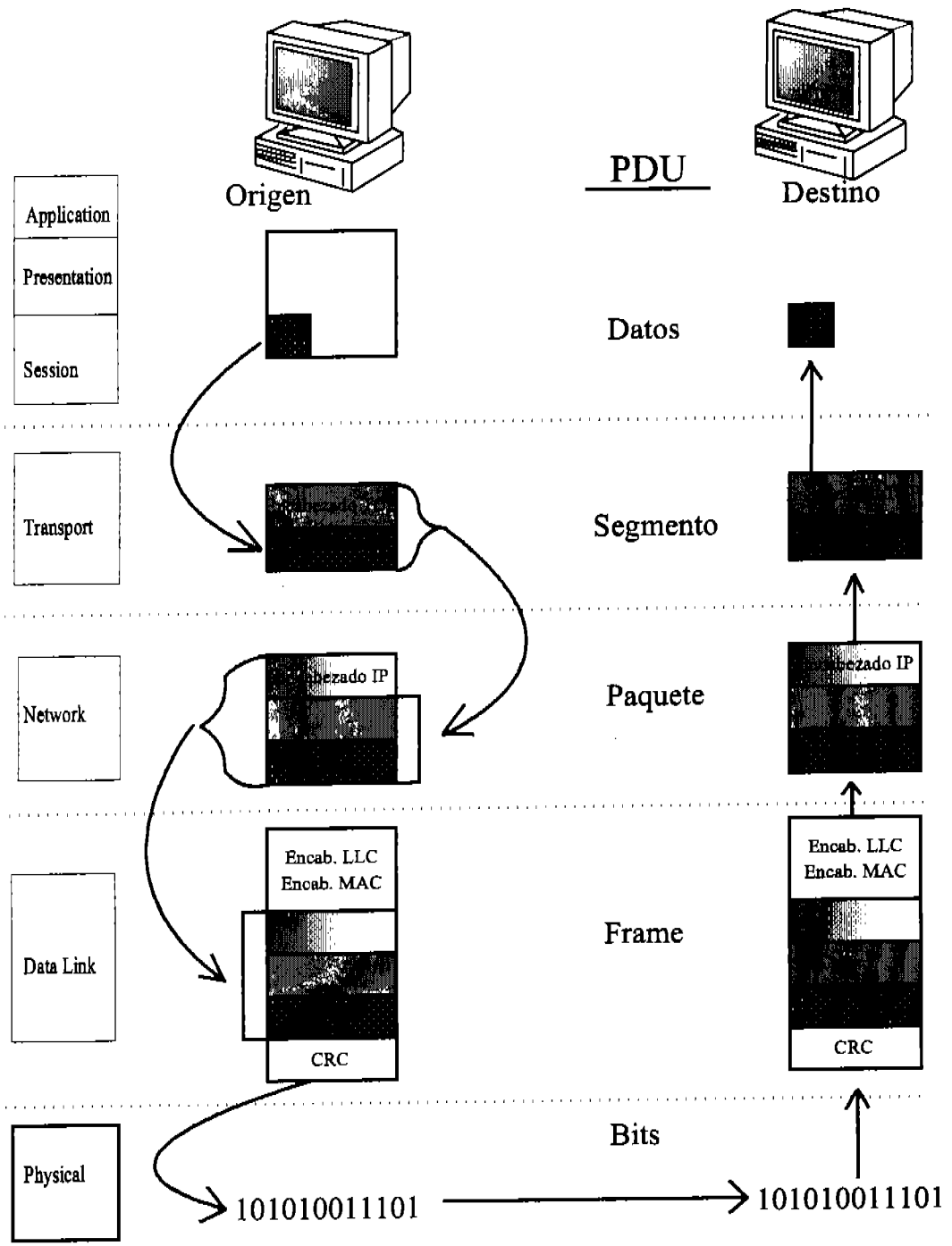


Figura 2.16 Encapsulamiento y desencapsulamiento.

- La siguiente capa, la capa de enlace de datos coloca lo recibido en el campo de datos de su PDU que se llama *Frame* o trama. Si la computadora de destino y la de origen se encuentran en la misma red local, esta capa añade el MAC de la computadora destino al encabezado del *Frame*, en caso de tratarse de una computadora remota añade el MAC de la puerta de salida

(normalmente la interfase del ruteador.) En el ejemplo considérese que se añade el MAC de la computadora de destino. Además de esto, se añade el MAC de origen y otros datos que LLC utiliza para establecer la conexión. Además del encabezado, en esta capa se añade al final de los datos un CRC de todo el *Frame*.

- Al llegar a la capa física, el *Frame* se descompone en *bit*s que a su vez se convierten en señales, que dependiendo del método de acceso al medio, se envían por la red.

- La capa física recibe las señales y las convierte en *bit*s que manda a la capa de enlace de datos. En esta capa, conforme se reciben los *bit*s se aplica un CRC, que se compara con el recibido al final del *Frame*. En caso de no ser iguales el *Frame* se deriva a tierra. También en esta capa se compara el MAC de destino con el propio en caso de no ser iguales también se desecha el *Frame*.

- Mientras la computadora de destino recibe los *Frames* y los procesa, dado que el método de transmisión es por *window*, el origen envía más *Frames*. (En este caso, otros dos, antes de esperar recibir un *Acknowledgment*.)

- Después de pasar por la capa de enlace de datos, los *Frames* se desencapsulan, es decir, el encabezado que ya se leyó se tira, quedando tan sólo lo que se conoce como paquete.

- El paquete se recibe por la capa de red y se lee el encabezado. Se compara el IP de destino con el propio y el CRC con el calculado por la capa, si alguno de estos no coincide el paquete se desecha. El encabezado se tira.

- La capa de transporte recibe y ordena los segmentos que van dirigidos al mismo puerto de destino y con el mismo puerto de origen. De esta manera se identifica (ya que en esta capa no se cuenta con IP o MAC) la computadora y la instancia de la aplicación de donde proviene el segmento. Como en el ejemplo la ventana tiene una longitud de tres, la capa de transporte espera a recibir tres segmentos antes de mandar un *Acknowledgment* positivo para pedir la siguiente ventana o, en caso de faltar alguno de los segmentos en la secuencia anterior, el segmento faltante.

- En el extremo emisor, en la capa de transporte, la copia de los segmentos que se han enviado se desecha al recibir el *Acknowledgment* que acredita que han llegado con bien al receptor.

- Este proceso sigue hasta terminar con toda la secuencia de segmentos que compone el archivo. En el extremo receptor, al tener todos los segmentos éstos se ordenan y se pasan a las capas superiores.

En la figura 2.17 se ilustra el sistema de direccionamiento que se utiliza en las diferentes capas.

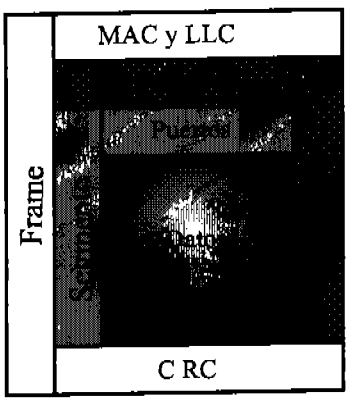


Figura 2.17 Direccionamiento en las diferentes capas. La longitud de las barras verticales abarca todos los elementos que contiene el PDU cuyo nombre llevan. Por ejemplo un paquete se compone de IP, puertos y datos o de IP y segmento ya que esos elementos son los que equivalen a la longitud de la barra vertical con el nombre "paquete".

Capítulo 3

Direccionamiento por IP

3.1 Introducción

Hoy en día, con la popularidad que gozan las redes computacionales, prácticamente cualquier persona envuelta en el medio ha tenido que poner un IP o conoce el IP del servidor que alberga su sitio de Internet favorito. Sin embargo, a pesar de esta exposición al tema, son pocas las personas que manejan eficientemente los diferentes aspectos del direccionamiento por IP. Algo seguro es que los certificados CCNA ¡sí lo hacen!

Es importante para comprender este capítulo manejar cómodamente la conversión numérica de una base a otra, en especial de decimal a binario y a hexadecimal.

3.2 Esquema Jerárquico del Direccionamiento IP

Un IP está formado por 32 *bit*s divididos en cuatro octetos y que normalmente representamos en una notación decimal punteada. Es importante tener en mente que el IP consiste en cuatro octetos binarios y tan sólo se representa con 4 números decimales separados por puntos. De este modo es fácil comprender la razón de que nunca se utilice un número mayor a 255 al asignar IP's: El número más grande que se puede obtener con 8 *bit*s es 11111111 que equivale a 255 en decimal.

El esquema de direccionamiento por IP es jerárquico, es decir para buscar un IP no se busca directamente ese IP sino que primero se busca la red que lo contiene y después el IP mismo.

Los IP's pueden ser públicos o privados. Los IP's públicos son asignados por la IANA de acuerdo a esquemas regionales y se tiene acceso a ellos a un nivel mundial, es decir que son visibles desde Internet. Los IP's privados son utilizados para ambientes LAN, que no accesan directamente a Internet. Aunque un administrador de LAN puede asignar prácticamente cualquier rango de IP's para su LAN, hay rangos preestablecidos para IP's privados. Estos rangos se utilizan para detectar paquetes que pudieran filtrarse accidentalmente a Internet desde una red privada y que por lo tanto solamente producirían tráfico basura.

Para lograr direccionar de una manera jerárquica los IP's a nivel mundial, cada IP se divide en dos partes: la primera especifica la red a la que pertenece el IP y la segunda parte especifica la máquina en particular dentro de dicha red. Estas partes son el *Net ID* y el *Host ID*. Véase la figura 3.1

Sin embargo, estas partes no siempre tienen la misma longitud en *bit*s, sino que son variables. Pero... ¿Cómo se puede determinar qué parte de una IP pertenece al *Net ID* y qué parte pertenece al *Host ID*? Para eso se utiliza la máscara de red.

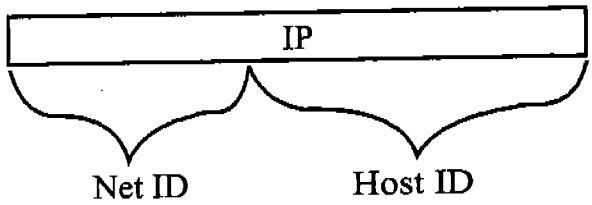


Figura 3.1 El IP se divide en dos partes: *Net ID* y *Host ID*.

La máscara de red es una sucesión de unos seguida de una sucesión de ceros que indica, precisamente, hasta qué *bit* en un IP pertenece al *Net ID*. Una manera de verlo es que el *Net ID* es el resultado de aplicar una And lógica al IP original y la máscara de red. Véase la figura 3.2

	Net ID	Host ID
IP	10100011.10001101.	00010010.11100010
Mascara	11111111.11111111.	00000000.00000000

Net ID 10100011.10001101. 00000000.00000000

Figura 3.2 Determinación del *Net ID* y del *Host ID* por medio de la máscara de red.

En el ejemplo de la figura 3.2, se puede apreciar que el *Net ID* es exactamente igual al IP original en los *bit*s correspondientes a los *bit*s prendidos en la máscara y a partir de allí, se complementa con ceros hasta tener 32 *bit*s.

Las redes se dividen en clases y según la clase a la que pertenece una red le corresponde una máscara por *default* y por consiguiente una diferente longitud de su IP será su *Net ID*. Las redes se clasifican según comienza su IP en binario. Véase la tabla 3.1

Clase de red	Primeros bits en el IP
Clase A	0
Clase B	10
Clase C	110
Clase D	1110
Clase E	1111

Tabla 3.1 Clases de redes de acuerdo a los primeros *bit*s en su IP.

Las redes con clases A, B y C se utilizan para asignar a organizaciones IP's de modo que sus computadoras se puedan comunicar en Internet directamente. Estas redes se asignan por bloques de IP's a las que se les refiere por medio de su *Net ID* y se asignan dependiendo del número de IP's necesarios. Las redes clase D se utilizan por la WWW para *multicast* y las redes clase E para experimentación.

En el direccionamiento por clases, la clase a la que pertenece el IP determina la porción del IP que es *Net ID* y la parte que es *Host ID*. Véase la figura 3.3

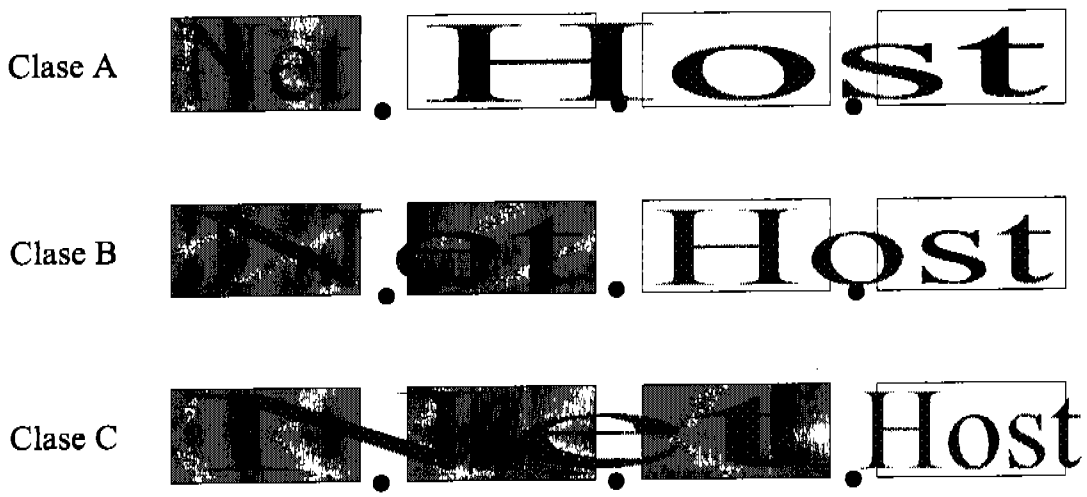


Figura 3.3 Net y *Host ID*'s según la clase del IP.

Implícitamente, las máscaras por *default* también dependen de la clase a la que pertenece el IP. Véase la figura 3.4

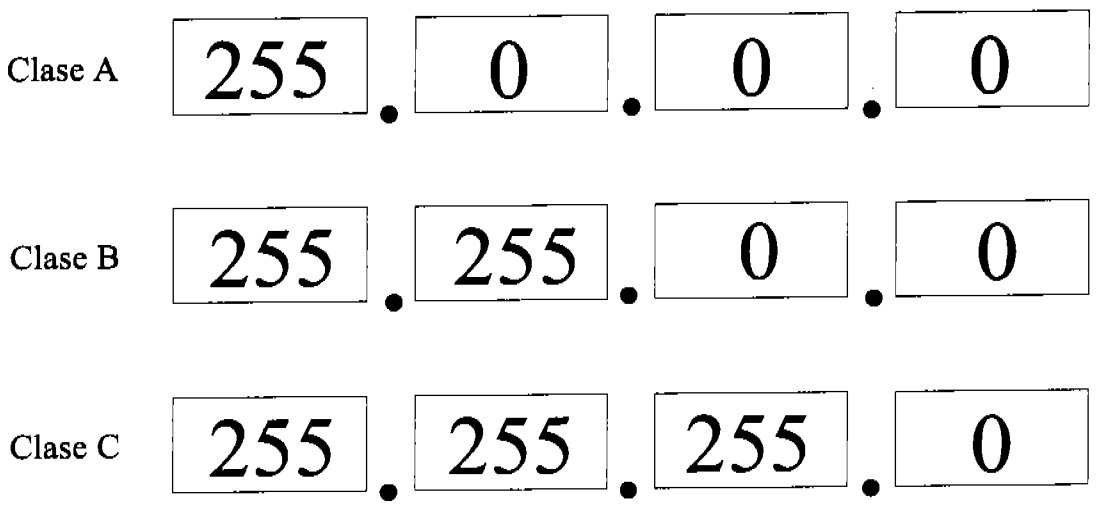


Figura 3.4 Máscaras de red por clase. Si los IP's clase A tienen un octeto para identificar la red y tres octetos para identificar los *hosts* en esa red, entonces hay relativamente pocas redes clase A con muchísimos IP's para *hosts* en cada una. De igual manera, se puede ver que en la clase B hay más redes que en la clase A pero cada una de estas redes tiene menos *hosts* que los que tienen las redes en la clase A, y que la clase C tiene muchas más redes que las otras dos clases pero también tiene el menor número de *hosts* por red de las tres clases.

Al asignar un IP a un dispositivo, hay que tener en cuenta tres reglas básicas:

- El IP no puede comenzar con el número 127. (Los IP's que comienzan con el 127 están reservadas para probar la configuración de TCP/IP en un *host* y se llaman direcciones de *loopback.*)
- La parte de *Net ID* no puede estar conformada, en binario, sólo por unos o sólo por ceros sino que necesariamente tiene que tener por lo menos un uno y un cero.
- El *Host ID* no puede estar conformado exclusivamente de ceros o de unos.

Considerando estas reglas y los *bit*s de inicio que definen a cada clase se puede hacer un análisis numérico por clase:

Los IP's clase A comienzan con 0 y el *Net ID* es el primer octeto por lo tanto el IP en binario de todas las redes clase A se podría representar en binario como se muestra en la figura 3.5.

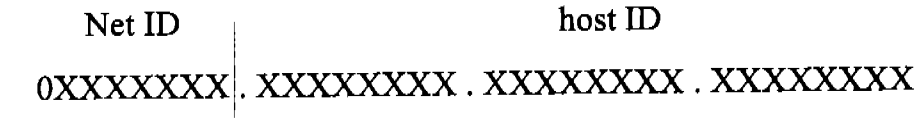


Figura 3.5 Representación de un IP clase A en donde las X representan *bit*s que pueden tener cualquier valor

Por análisis combinatorio sabemos que si el *Net ID* tiene 7 *bit*s variables con dos valores posibles cada uno, hay 2^7=128 maneras de satisfacer este esquema. Sin embargo, una de estas combinaciones es 00000000 lo cual no es válido por tener solamente ceros en todo el *Net ID* y otra combinación es 01111111 que es el número 127 y no se puede tener una IP que comience con ese número. De modo que, hay exactamente 2^7-2 combinaciones posibles para un *Net ID* clase A o, dicho de otro modo, hay 126 redes clase A.

Otro dato que el análisis muestra en cuanto a las redes clase A es que el número válido más pequeño para el primer octeto es 1 y número más grande 126. Por lo tanto se sabe que cualquier IP cuyo primer octeto se encuentre en el rango 1-126 en decimal, corresponde a un octeto en binario que comienza con cero y cumple con las reglas de asignación de IP's.

Cada una de las 126 redes clase A tiene 24 *bit*s para albergar a sus respectivos *hosts* por lo que puede albergar a 2^{24}-2 *hosts.* (En este caso se restan dos porque una combinación se compone de puros ceros y otra de puros unos, lo que no es válido para un IP asignable a un *host.*) Análogamente se puede hacer un análisis para cada una de las clases de redes. Véase la tabla 3.2.

Clase de red	Primeros bits	Rango del 1er Octeto en dec.	Número de redes	Número de Hosts por red
A	0	1-126	2^7-2 =126	2^{24}-2 =16,777,214
B	10	128-191	2^{14} =16,384	2^{16}-2 =65,534
C	110	192-223	2^{21} =2,097,152	2^8-2 =254
D	1110	224-239	No hay	No hay
E	1111	240-255	No hay	No hay

Tabla 3.2 Análisis numérico de las clases de redes.

Es importante aclarar que el *Net ID* identifica una red completa y por lo tanto no tiene que ser una dirección IP válida para asignar a un *host* en particular. De hecho, como ya se habrá visto, todo *Net ID* tiene en la parte de *host* solamente ceros. Esto no cumple con las reglas para asignación de IP's pero eso está bien ya que el *Net ID* no se asigna a dispositivo alguno sino que es sólo un identificador, un nombre de toda la red. Cuando dos dispositivos tienen IP's que señalan hacia el mismo *Net ID*, de inmediato se sabe que dichos dispositivos se encuentran en la misma red y que se ven entre ellos de manera directa.

Ejercicio 3.1

Para cada IP dado, determinar la clase a la que pertenece, la máscara de red, el *Net ID* y el *Host ID*.

IP del dispositivo	Clase	Mascara de red	Net ID	Host ID
129.23.123.9	B	255.255.0.0	129.23.0.0	123.9
245.5.9.123	E	----	----	----
192.57.23.87	C	255.255.255.0	192.57.23.0	87
1.1.76.18	A	255.0.0.0	1.0.0.0	57.23.87
0.12.5.7	----	----	----	----
224.234.210.78	D	----	----	----
130.65.17.74	B	255.255.0.0	130.65.0.0	17.74
90.34.90.34	A	255.0.0.0	90.0.0.0	34.90.34
12.6.34.9	A	255.0.0.0	12.0.0.0	6.34.9
120.128.129.130	A	255.0.0.0	120.0.0.0	128.129.130
128.120.123.130	B	255.255.0.0	128.120.0.0	123.130
254.8.8.8	E	----	----	----
193.123.43.89	C	255.255.255.0	193.123.43.0	89

Ejercicio 3.1

Ejercicio 3.2

Determinar si es posible asignar los siguientes pares de IP's a un par de computadoras que se encuentran en la misma red.

- 12.23.90.2
  12.100.134.0
  Sí es posible ya que son IP's válidos y el *Net ID* en ambos casos es el mismo: 12.0.0.0.

- 194.12.59.21
  194.12.57.22
  No es posible porque sus *Net ID*'s son diferentes.

- 224.12.15.1
  224.12.15.2
  No es posible porque son IP's clase D.

- 45.12.90.6
  45.12.90.6
  No es posible porque son exactamente el mismo IP y no puede haber dos IP's iguales en la misma red.

- 145.134.98.23
  145.134.1.0
  Sí es posible.

- 10.100.200.255
  10.1.2.3
  Sí es posible.

- 200.34.60.0
  200.34.60.1
  No es posible porque el *Host ID* de uno de ellos está compuesto solamente por ceros.

- 5.90.271.23
  5.45.23.0
  No es posible porque uno de los números no es representación de un octeto binario.

- 5.8.0.0
  5.0.9.0
  Sí es posible (Aunque hay muchos ceros, los *host* y *Net ID*'s no están compuestos exclusivamente de ceros.)

3.2.1 Rango de direcciones públicas y privadas

Las direcciones IP, como se mencionó en la sección anterior, se dividen en direcciones públicas y direcciones privadas. Las direcciones públicas y los rangos de direcciones privadas, que se manejan en el ámbito de las LANs, son asignadas por la IANA.

Las IP's privadas permiten la conectividad y direccionamiento en redes cuyas computadoras no necesitan salir a Internet con su propio IP. Si cada computadora que alguna vez necesita salir a Internet necesitara una IP pública, simplemente no habría suficientes IP's. Al utilizar rangos privados de redes, las máquinas que tienen IP's privados todavía pueden salir a Internet por medio de algún tipo de NAT y no ocupan permanentemente un IP público.

Hay un rango de direcciones privadas para cada clase de redes. Véase la tabla 3.3

Clase de red	Rango reservado para direcciones privadas
A	10.0.0.1 hasta 10.255.255.254
B	172.16.0.1 hasta 172.31.255.254
C	192.168.0.1 hasta 192.168.255.254

Tabla 3.3 Rango de IP's privadas.

Al configurar una red privada es importante utilizar uno de estos rangos porque aunque otros rangos pueden funcionar, estos rangos no generan tráfico en Internet. Considerando las capacidades discutidas en la sección anterior es fácil elegir la clase adecuada para el rango de una red privada. Sin embargo, ya que no hay costos adicionales por elegir una red más grande, siempre que se prevea crecimiento en la red, es buena norma optar por el rango privado en la clase A.

3.2.2 *Broadcast*

Se ha utilizado el término *broadcast* constantemente en los capítulos 1 y 2. Sin embargo, es hasta este punto que se puede definir un último detalle al respecto. Mientras que el *broadcast* en capa dos es una dirección física en la que toda la dirección consiste solamente en unos en binario y normalmente se representa como FF-FF-FF-FF-FF-FF en hexadecimal, el *broadcast* en capa tres es bastante más complejo ya que no siempre es el mismo para todas las redes en donde se emplea.

El *broadcast* capa tres es único para la red en la que se encuentra y se obtiene al tomar el *Net ID* y en lugar de sustituir la parte de *host* con ceros, se sustituye con unos.

Recapitulando, el *Net ID* no es un IP válido para asignar a un *host* porque la parte correspondiente al *host* en el IP esta llena sólo de ceros y el *broadcast* de capa tres tampoco es un IP válido para asignar a un dispositivo en particular porque esa parte esta llena tan sólo de unos.

Cada red, entonces, se identifica con un IP reservado al principio de ésta este IP es el *Net ID* y al final de la red hay otro IP reservado que es el *broadcast* y significa "Todos los dispositivos en esta red". Véase la figura 3.6

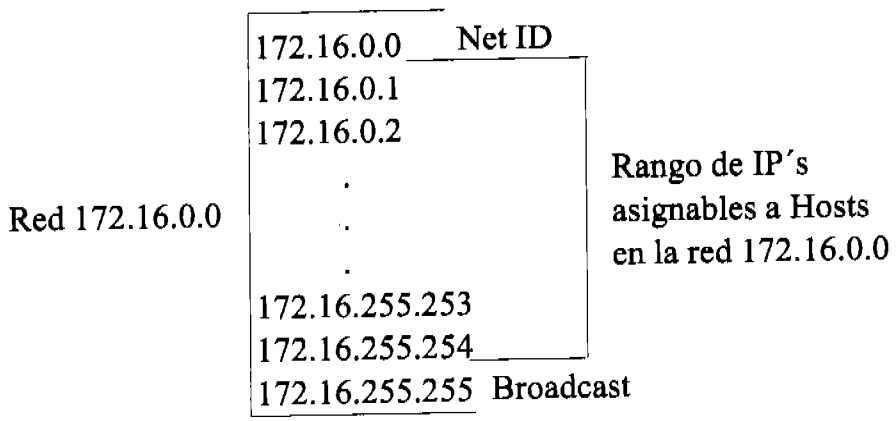


Figura 3.6 Ejemplo de una red con su *Net ID* y su *broadcast*.

3.3 Creación de Sub-redes

En el esquema de direccionamiento por clases, es fácil determinar el número de *hosts* en una red directamente por la clase a la que pertenece. Sin embargo, la necesidad de tener más redes públicas y un mejor manejo de las redes privadas hacen que este tipo de direccionamiento sea insuficiente.

En una red de miles de nodos, sin duda es una buena idea organizar el tráfico entre las máquinas. Pero al tener una sola red, cada *broadcast* se envía a cada uno de los dispositivos que se encuentran en ella, lo que crea una gran cantidad de tráfico muchas veces innecesario.

Si la misma red se divide por departamentos de unas cuantas decenas de computadoras cada uno y entre los distintos departamentos se introducen ruteadores, esto disminuirá enormemente el tráfico en la red ya que los ruteadores rompen los dominios de *broadcast*, así que los *broadcasts* se transmitirán tan sólo a las computadoras del mismo departamento y no a todas las computadoras de la red.

Los segmentos de red separados por ruteadores se llaman sub-redes. Ahora se necesita un esquema que permita identificar sub-redes dentro de la misma red y esto se consigue dividiendo el rango completo de la red en rangos más pequeños, sub-redes, y reservando, en cada sub-red al principio y al final de esta una dirección para *Net ID* y para *broadcast* respectivamente de la sub-red en particular. A esto se le llama *subnetting*.

El *subnetting* provee varios beneficios entre los cuales están una mayor flexibilidad, limitar el tráfico causado por *broadcasts* y uso más eficiente de las direcciones IP en una red.

Así como en una red por clase se contaba con una máscara de red que definía la porción del IP que correspondía al *Net ID*, para dividir una red en sub-redes se utiliza una máscara de sub-red.

Al igual que la máscara de red, la máscara de sub-red es una sucesión de unos seguida de una sucesión de ceros y la porción del IP correspondiente a los *bit*s prendidos en la máscara es el *Net ID*, pero a diferencia de ésta, la máscara de sub-red no está predeterminada ni es fija para cada clase de redes. Más bien, la máscara de sub-red se determina por el administrador de la red para satisfacer las necesidades numéricas en la sub-red que la aplique.

La máscara de sub-red puede tomar cualquier valor que cumpla con la condición de tener una sucesión de unos seguida de una sucesión de ceros, incluyendo series de unos que no coincidan con el término de un octeto entero. De ese modo, en lugar de los dos únicos valores que podía tomar un octeto en la máscara de red (0 ó 255), en la máscara de sub-red los octetos pueden tomar los siguientes valores: 0, 128, 192, 224, 240, 248, 252, 254 y 255. Véase la tabla 3.4.

Valor en binario que puede ser parte de una serie de unos seguida de una serie de ceros	**Valor equivalente en decimal**
0 0 0 0 0 0 0 0	0
1 0 0 0 0 0 0 0	128
1 1 0 0 0 0 0 0	192
1 1 1 0 0 0 0 0	224
1 1 1 1 0 0 0 0	240
1 1 1 1 1 0 0 0	248
1 1 1 1 1 1 0 0	252
1 1 1 1 1 1 1 0	254
1 1 1 1 1 1 1 1	255

Tabla 3.4 Valores que pueden tomar los octetos de una sub-máscara de red

Una dirección de sub-red se crea tomando *bit*s de la parte de *host* según la máscara de sub-red que se emplee. Los *bit*s que se toman de la parte de *host* se convierten en la parte de sub-red. En la figura 3.7 se muestra un ejemplo al tomar el IP 172.16.85.9 y determinar su *Net ID* y su *Host ID* con la máscara por *default* según su clase. En la parte baja de la figura, se muestran los nuevos *Net ID* y *Host ID* al utilizar (arbitrariamente) tres *bit*s que pertenecían a la parte de *host* para formar la parte de sub-red. La sub-máscara de red se asignó arbitrariamente en este ejemplo pero es fácil ver que ésta dependerá del número de redes que se desee obtener después de aplicar el *subnetting*. Véase la figura 3.7

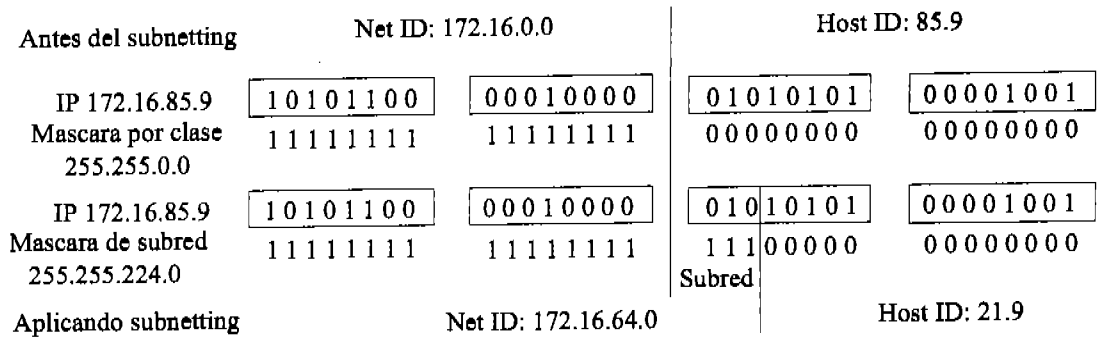


Figura 3.7 Ejemplo de aplicación de *subnetting*.

Nótese en el ejemplo, que la parte de sub-red indica que tres *bit*s más pasan a formar parte del *Net ID*.

Las reglas para asignar un IP a un dispositivo antes de utilizar *subnetting* eran:

- El IP no puede comenzar con el número 127.
- El *Net ID* no puede estar compuesto sólo de unos o sólo de ceros.
- El *Host ID* no puede estar compuesto sólo de unos o sólo de ceros.

Al asignar un IP a un dispositivo utilizando una sub-máscara de red se añade una regla más al conjunto:

- La parte de la IP que se convierte en sub-red no puede estar compuesta sólo de unos o sólo de ceros.

3.3.1 CIDR (*Classless Inter-Domain Routing*)

A este método en el que se aplican sub-máscaras de red en lugar de máscara por clase que corresponde a una IP según su primer octeto se le llama CIDR (*Classless Inter-Domain Routing*.) CIDR tiene su propia notación, que asocia una máscara de red con un IP. En la notación CIDR simplemente se agrega al IP original una diagonal con el número de *bit*s encendidos en la sub-máscara de red.

Por ejemplo, el IP 20.120.56.230 con sub-máscara de red 255.255.240.0, se puede representar en notación CIDR como 20.120.56.230/20 ya que la sub-máscara de red 255.255.240.0 es equivalente a 11111111.11111111.11110000.00000000 que es una sucesión de 20 unos seguida de ceros.

El método de asignación de IP´s por clases es un método sencillo, con el que se puede diferenciar de manera rápida un *host* local de uno remoto y en el caso del *host* remoto, la ruta para llegar a él. Sin embargo, este método permite muy pocas variaciones en el tamaño de las redes. El método no basado en clases CIDR permite optimizar el uso de las IP´s al manejar sub-redes que pueden variar en tamaño según la sub-máscara de red que se les aplique. La tabla 3.5 muestra las Sub-máscaras de

red en notación decimal punteada, su correspondiente representación en CIDR y una equivalencia en términos de redes por clase. Véase la tabla 3.5

sub-máscara en notación decimal punteada	sub-máscara en notación CIDR	Equivalencia en tamaño a redes por clase.
255.0.0.0	/8	256 redes clase B o 1 red clase A
255.128.0.0	/9	128 redes clase B
255.192.0.0	/10	64 redes clase B
255.224.0.0	/11	32 redes clase B
255.240.0.0	/12	16 redes clase B
255.248.0.0	/13	8 redes clase B
255.252.0.0	/14	4 redes clase B
255.254.0.0	/15	2 redes clase B
255.255.0.0	/16	1 red clase B o 256 redes clase C
255.255.128.0	/17	128 redes clase C
255.255.192.0	/18	64 redes clase C
255.255.224.0	/19	32 redes clase C
255.255.240.0	/20	16 redes clase C
255.255.248.0	/21	8 redes clase C
255.255.252.0	/22	4 redes clase C
255.255.254.0	/23	2 redes clase C
255.255.255.0	/24	1 red clase C
255.255.255.128	/25	½ de red clase C
255.255.255.192	/26	¼ de red clase C
255.255.255.224	/27	1/8 de red clase C
255.255.255.240	/28	1/16 de red clase C
255.255.255.248	/29	1/32 de red clase C
255.255.255.252	/30	1/64 de red clase C

Tabla 3.5 Equivalencia por tamaño de redes entre CIDR y redes por clase.

Al utilizar CIDR, se crean sub-redes y al crearlas, algunos IP's que eran válidos para asignar a un *host* se utilizan para nombrar toda la sub-red y por lo tanto ya no se pueden asignar a un dispositivo.

Véase el ejemplo en la figura 3.8. En este ejemplo se muestra la red 172.16.0.0 subdividida con una sub-máscara /24. Nótese que cuando la parte del IP correspondiente al *Host ID* y la parte correspondiente a la sub-red son puros ceros, entonces se tiene un identificador de red por clase. En el caso en el que el *Host ID* esta formado sólo por ceros y la parte de sub-red es válida se trata de un identificador de sub-red y en el caso en que la parte de *host* está formada solamente por unos, entonces se trata del *broadcast* de la sub-red correspondiente. Las sub-redes en que la parte de la sub-red está compuesta sólo de unos o sólo de ceros, no son utilizables (por lo menos para propósitos del examen.)

En este ejemplo se eligió una sub-máscara de red que coincide con un octeto entero (/24) para facilitar la visualización de los identificadores de sub-redes y sus *broadcasts*.

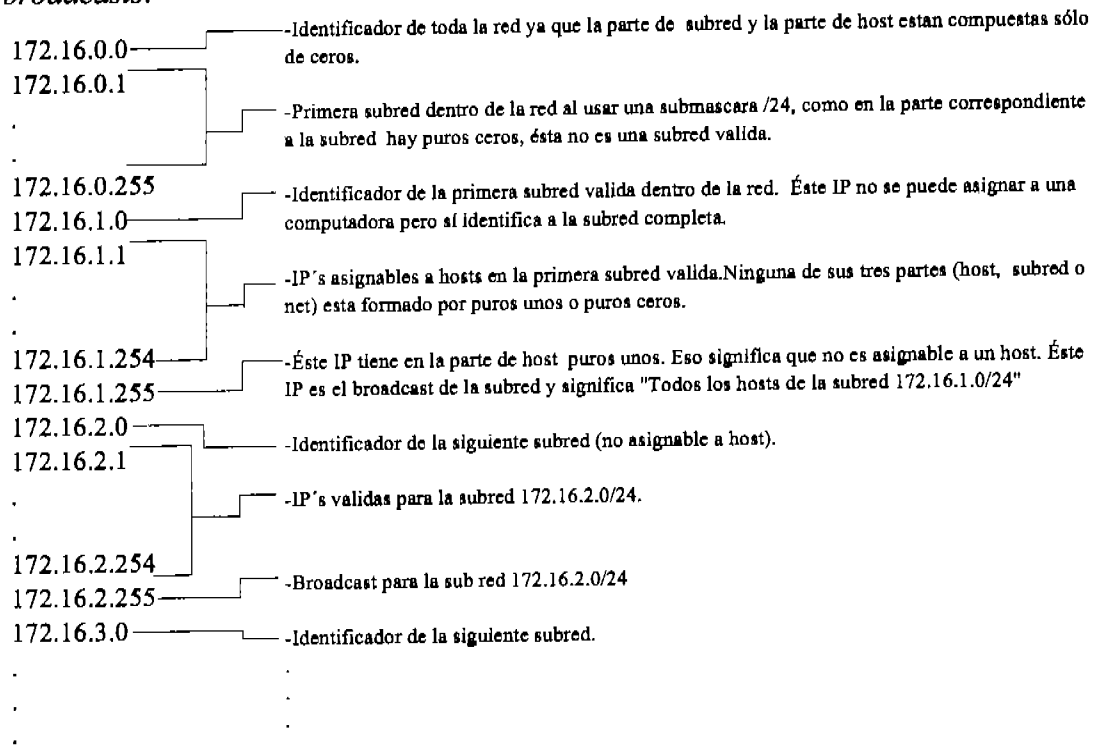


Figura 3.8 Ejemplo de la subdivisión de la red 172.16.0.0 en sub-redes máscara /24

Nótese que el primer IP de toda la red es el identificador de la red entera, y en cada sub-red el primer IP es el identificador de la sub-red y el último IP es el *broadcast* de la sub-red. Los IP´s asignables a *hosts* son los que se encuentran en el rango que va desde un IP más que el identificador de sub-red (*Net ID* para la sub-red) hasta un IP menos que el *broadcast* para la sub-red. Nótese también que el IP siguiente a un *broadcast* es el *Net ID* de la siguiente sub-red.

Ejercicio 3.3

Determinar, para cada uno de los siguientes IP´s con sub-máscara en notación CIDR, si son o no válidos para asignar a una computadora, cuál es su *Net ID*, su *Host ID*, su *broadcast*, el número de sub-redes que genera la sub-máscara, el número de *hosts* que se pueden asignar dentro de cada sub-red y el rango de IP´s asignables a *hosts* en la sub-red a la que pertenece el IP dado.

- 214.65.23.4/27

  Convirtiendo el IP y su sub-máscara a binario:

  11010110 . 01000001 . 00010111 . 000 00100
  11111111 . 11111111 . 11111111 . 111 00000
  subred

  Por tratarse de un IP clase C su máscara de red cubre los tres primeros octetos (/24.) Y, dada la máscara de sub-red /27 hay tres *bits* en la parte de sub-red (*bits* 25, 26 y 27) los cuales, en este caso, están en cero.

  Por lo tanto, como la parte de sub-red esta compuesta solamente por ceros, el IP no es asignable a un *host*.

- 12.93.156.172/20

  en binario:

  00001100 . 01011101 . 1001 1100 . 10101100
  11111111 . 11111111 . 1111 0000 . 00000000
  red subred host

  - En este caso, el IP corresponde a una clase A por lo tanto, la parte de red llega hasta el primer octeto. De allí en adelante, los unos en la sub-máscara determinan la parte de sub-red del IP.

  Por lo tanto, este IP sí es válido para asignarlo a un *host*.

  - El *Net ID* es la parte del IP que tiene unos debajo y está compuesto por las partes del IP para la red y la subred y con ceros en la parte de *host*. En otras palabras el *Net ID* sigue siendo una And lógica del IP con la máscara.

  El *Net ID* es 00001100 . 01011101 . 1001 0000 . 00000000 es decir: 12.93.144.0.

  - El *Host ID* es la parte del IP que tiene ceros debajo: 1100 . 10101100 ó sea: 12.172.

  - El *broadcast* se forma por la parte de red y de sub-red pero en lugar de sustituir la parte de *host* con ceros como se hizo para obtener el *Net ID*, se sustituye por unos:

  00001100 . 01011101 . 1001 1111. 11111111 = 12.93.159.255.

- El número de sub-redes se determina por el número de combinaciones posibles con los *bits* en la parte de sub-red menos dos (por la combinación en que hay puros ceros y en la que hay puros unos):

Como hay 12 *bits* en la parte de sub-red, con esa sub-máscara de red se obtienen 2^{12}-2 = 4094 sub-redes de una red clase A.

- El número de *hosts* en cada una de las 4094 sub-redes se determina por el número de *bits* en la parte de *host*.

Hay 2^{12}-2= 4094 *hosts* en cada una de las 4094 sub-redes.

- El rango de IP's asignables en la sub-red que contiene a la IP dada es desde el *Net ID* más uno hasta el *broadcast* menos uno:

El rango válido va desde 12.93.144.1 hasta 12.93.159.254

- 129.15.18.39/26

En este ejemplo se divide directamente el IP con los datos de la máscara pero sin poner la máscara en binario explícitamente (Es bueno buscar atajos porque el tiempo es uno de los principales factores al tomar el examen):

10000001 . 00001111	. 00010010 . 00	100111
red	**subred**	**host**

-El IP es válido. (No hay parte alguna con ceros o unos exclusivamente)

-El *Net ID* es 10000001.00001111.00010010.00000000 = 129.15.18.0

-El *Host ID* es 100111 = 39

-El *broadcast* es 10000001.00001111.00010010.00111111 = 129.15.18.63

-Con ésta máscara se tienen 2^{10}-2 = 1022 sub-redes.

-Con ésta máscara se tienen 2^{6}-2 = 62 *hosts* en cada una de las 1022 sub-redes.

-El rango de IP's válidos alrededor de la IP dada es: de 129.15.18.1 a 129.15.18.62.

- **200.29.15.42/29**

11001000 . 00011101 . 00001111	. 00101	010
red	subred	host

-Sí es un IP válido.

-Su *Net ID* es 11001000.00011101.00001111.00101000 = 200.29.15.40

-EL *Host ID* es 010 = 2

-El *broadcast* es 11001000.00011101.00001111.00101111 = 200.29.15.47

-El número de sub-redes, 2^5-2 = 30

-El número de *hosts* es 2^3-2 = 6 en cada sub-red.

-El rango de IP's válidas en la sub-red donde se encuentra ese IP es: desde 200.29.15.40 hasta 200.29.15.47

- **36.15.18.143/22**

-Válido.

-El *Net ID* es 36.15.16.0

-El *Host ID* es 2.143

-El *broadcast* es 36.15.19.255

-El número de sub-redes es 16382

-El número de *hosts* por sub-red, 1022

-El rango va de 36.15.16.1 a 36.15.19.254

- **195.48.52.18/27**

-No es válido

- 203.43.18.69/26

  -Sí es válido.

  -*Net ID*: 203.43.18.64

  -*Host ID*: 5

  -*Broadcast*: 203.43.18.127

  -Sub-redes: 2

  -*Hosts* por sub-red: 62

  -Rango: de 203.43.18.65 a 203.43.18.126

Haciendo un análisis numérico similar al que se hizo con las redes por clases, se puede determinar el número de sub-redes y el número de *hosts* por sub-red para cada sub-máscara posible en cada clase. Véanse las tablas 3.6, 3.7 y 3.8

Clase A				
sub-mascara	**Bits en sub-red**	**Bits en host**	**No. sub-redes**	**No. hosts**
/9	No es usable para el examen de Cisco.			
/10	2	22	2	4194302
/11	3	21	6	2097150
/12	4	20	14	1048574
/13	5	19	30	524286
/14	6	18	62	262142
/15	7	17	126	131070
/16	8	16	254	65534
/17	9	15	510	32766
/18	10	14	1022	16382
/19	11	13	2046	8190
/20	12	12	4094	4094
/21	13	11	8190	2046
/22	14	10	16382	1022
/23	15	9	32766	510
/24	16	8	65534	254
/25	17	7	131070	126
/26	18	6	262142	62
/27	19	5	524286	30
/28	20	4	1048574	14
/29	21	3	2097150	6
/30	22	2	4194302	2
/31	No es utilizable.			

Tabla 3.6 Número de sub-redes y de *Hosts* para una clase A con CIDR

Clase B				
sub-mascara	Bits en la parte de sub-red	Bits en host	No. sub-redes	No. hosts
/17	No es usable para el examen de Cisco.			
/18	2	14	2	16382
/19	3	13	6	8190
/20	4	12	14	4094
/21	5	11	30	2046
/22	6	10	62	1022
/23	7	9	126	510
/24	8	8	254	254
/25	9	7	510	126
/26	10	6	1022	62
/27	11	5	2046	30
/28	12	4	4094	14
/29	13	3	8190	6
/30	14	2	16382	2
/31	No es utilizable.			

Tabla 3.7 Número de sub-redes y de *hosts* para una clase B con CIDR

Clase C				
sub-mascara	Bits en sub-red	Bits en host	No. sub-redes	No. hosts
/25	No es válido para el examen de Cisco.			
/26	2	6	2	62
/27	3	5	6	30
/28	4	4	14	14
/29	5	3	30	6
/30	6	2	62	2
/31	No es utilizable.			

Tabla 3.8 Número de sub-redes y de *hosts* para una clase C con CIDR

Ejercicio 3.4

Asignar la máscara a la red 150.120.0.0 para tener 70 sub-redes o más con el mayor número de *hosts* por sub-red.

Para tener 70 sub-redes, se necesita que la parte de sub-red del IP tenga suficientes *bits* para albergarlas. Y, como se pide el mayor número de *hosts* posibles por sub-red, también se necesita que el número de *bits* que tenga la parte de sub-red sea el menor posible.

Con 7 *bits* se pueden tener $2^7-2=$ 126 combinaciones y con 6 *bits*, $2^6-2=$ 62 combinaciones. Así que, la cantidad mínima indispensable de *bits* para tener 70 sub-redes es 7. Como se trata de una red clase B y sí se considera la parte de sub-red con

7 *bits*, entonces la sub-máscara de red tiene que ser de 16 *bits* (por ser clase B) más 7 *bits* (para las 70 sub-redes.) La máscara que se busca es /23. Véase la figura 3.9

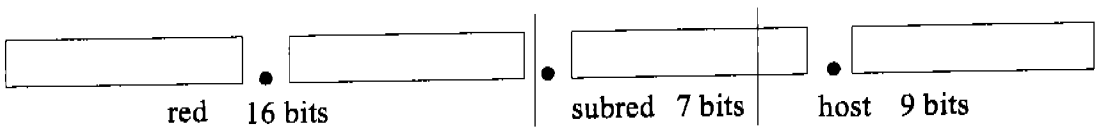


Figura 3.9 Subdivisión de una red clase B para albergar 70 redes y el máximo de *hosts*

Este resultado se puede comprobar en la tabla 3.7.

Ejercicio 3.5

Determinar el número de sub-redes en que se puede dividir una red clase B, si se desea tener exactamente 510 *hosts* en cada una de ellas.

2^9-2= 510 por lo tanto se necesitan 9 *bits* para la parte de *host*.

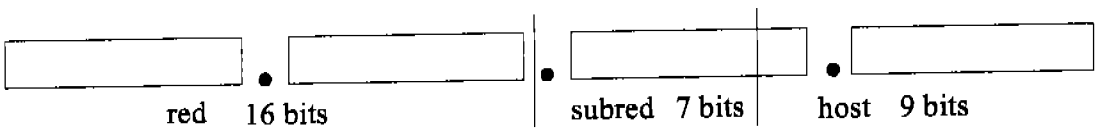


Figura 3.10 Subdivisión de una red clase B para que cada red tenga exactamente 510 IP's.

Nótese que la figura 3.11 es la misma que la figura 3.10 y, por supuesto esto es lógico. Al tener 9 *bits* en la parte de *host*, se tienen 7 *bits* en la parte de sub-red y por consiguiente 2^7-2 = 126 sub-redes.

Por lo tanto, el número de sub-redes en que se puede dividir una red clase B para tener exactamente 510 *hosts* en cada una es 126.

Ejercicio 3.6

Al aplicar CIDR a un IP en la tercer red privada clase C, éste se convierte en el duodécimo *host* válido de la duodécima sub-red válida. Encontrar ese IP y su máscara de sub-red.

Para empezar, el rango de redes privadas clase C es de 192.168.0.0 hasta 192.168.255.254. Y, como la máscara por *default* para la red es 255.255.255.0, entonces los tres primeros octetos determinan la red. Por lo tanto, la tercera red privada clase C es 192.168.2.0 (¿por qué 2 y no 3? - La primera red es la 192.168.0.0 y como la parte de red abarca los tres primeros octetos no hay problema en que el tercer octeto esté compuesto exclusivamente de ceros ya que los otros dos hacen la parte de red válida.)

Como la parte de sub-red alberga por lo menos 12 sub-redes, está tiene por lo menos 4 *bits* y como la parte de *host* que se busca tiene por lo menos 12 combinaciones, se

sabe que ésta tiene por lo menos 4 *bits*. La única posibilidad, entonces es que el octeto restante se divida en dos partes de cuatro *bits* cada una.
Por último, se sabe que la sub-red es la duodécima válida en la red por lo tanto en la parte de la sub-red se tendrá el número 12 en binario (en este caso no se comienza por 1 a red cero por que ésta no es válida.) También el *host* es el duodécimo y también en este caso, el *host* cero no es valido así que en la parte de *host* simplemente se pone el 12 en binario.

192	168	2	(12)	(12)
11000000 .	10101000 .	00000010	. 1100	1100
	Red		Subred	Host

La única máscara posible es /28 y, al leer este número binario, se tiene el IP que se busca: 192.168.2.204/28.

3.4 Mi Método para CIDR

Ya se mencionó la importancia del tiempo al tomar el examen. En el caso de *subnetting*, no es suficiente responder correctamente las preguntas, hay que hacerlo también muy rápidamente. Dependiendo del número de preguntas en el examen (es variable), se cuenta con aproximadamente minuto y medio por pregunta.

Es importante comprender el método binario y los conceptos generales de *subnetting* antes de utilizar este método, ya que aunque es mucho más rápido y más fácil, puede prestarse a ser utilizado de manera mecánica, sin entender realmente las preguntas. ¡Los examinadores de Cisco no son tan fáciles de complacer! Sin embargo, si se sabe perfectamente lo que esta sucediendo en binario, este método es una muy buena herramienta para el examen.

Antes de presentar el método, que depende del uso de tres sencillas tablas, cabe aclarar que no es posible ingresar al salón de examen con tabla alguna (o calculadora o reloj o teléfono o papeles) pero es perfectamente válido utilizar la pizarra de examen que el aplicador provee.

Vale la pena utilizar algunos minutos para generar las tres tablas ya que ellas serán útiles para todo el examen. Y es muy, muy importante generarlas correcta y nítidamente; llegar a medio examen y darse cuenta que se ha estado usando una tabla con un error ha de ser una experiencia demasiado abrumadora como para resolver sin distracciones la otra mitad del examen.

Las tablas que se deben aprender se presentan en la tabla 3.9 y son: una tabla de conversión, una tabla condensada de sub-redes y una tabla de n contra 2^n-2 para cálculo de combinaciones con determinado número de *bits*. Véase la tabla 3.9

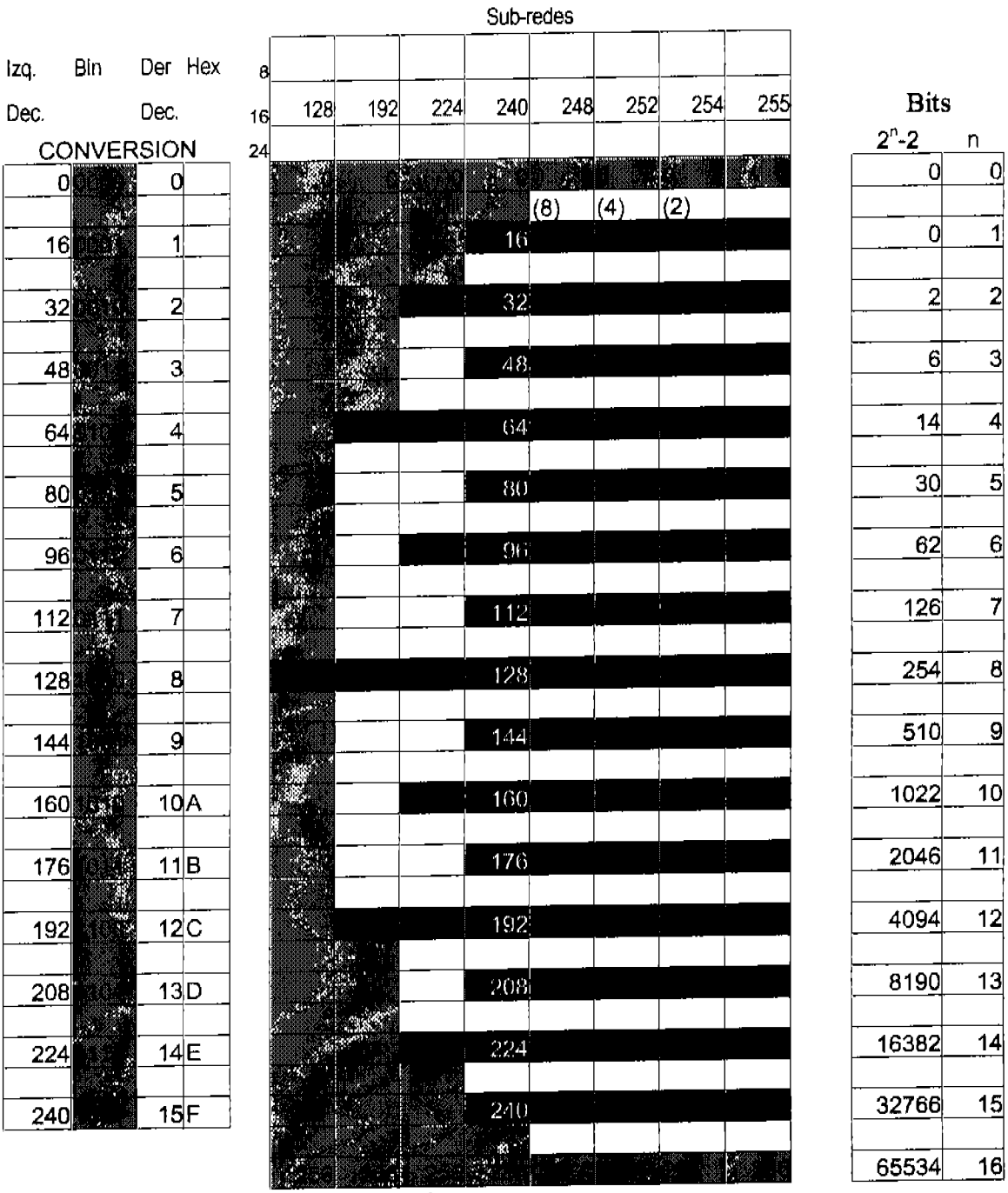


Tabla 3.9 Tablas de ayuda para *subnetting*.

3.4.1 Tabla de conversión

La tabla de conversión en la tabla 3.9 se compone de cuatro columnas: la primera es una cuenta en decimal de 16 en 16, la segunda es una cuenta en binario de cuatro *bit*s con incrementos unitarios, la tercera es una cuenta en decimal de uno en uno y

la cuarta es una cuenta en hexadecimal también de uno en uno (como los primeros diez números son iguales en decimal que en hexadecimal sólo se ponen a partir de A en hexadecimal)

Esta tabla se basa en el hecho de que para *subnetting* no se requiere cambiar de base ningún número mayor a un octeto en binario. La manera más rápida para cambiar de base de decimal a binario o viceversa es aprenderse las 256 combinaciones posibles en binario y sus equivalentes en decimal. este método es, obviamente, demasiado difícil y susceptible de errores. Pero, en el mismo tenor, no es tan difícil aprenderse las 32 combinaciones posibles al dividir el octeto en dos mitades, la mitad izquierda que varía de 16 en 16 y la mitad derecha que varía de uno en uno y después sumar las dos mitades.

Para el caso de la conversión a hexadecimal se utiliza la propiedad de que $2^4 = 16$. Entonces, cada cuatro *bit*s se pueden representar por un número hexadecimal así que tan sólo es necesario relacionar el número que se busque con la columna de la derecha.

Es recomendable saber generar la tabla sin errores pero es preferible aprenderla de memoria y saber convertir números a distintas bases mentalmente.

Ejercicio 3.7

Cambiar los siguientes números a sus equivalentes en decimal, binario o hexadecimal según haga falta.

- 10101001_2

  Para encontrar la equivalencia en decimal, Se divide el octeto en dos mitades 1010 que en la mitad izquierda corresponde a 160 y se suma a 1001 que en la mitad derecha corresponde a 9.

  Para hallar el número en hexadecimal, simplemente se busca la correspondencia de cada mitad con la columna de la extrema derecha. 1010 corresponde a A y 1001 a 9.

  $10101001_2 = 169_{10} = A9_{16}$

- 141_{10}

  El número más cercano en la columna izquierda es el 128 que en la de binario corresponde a 1000 y en la de hexadecimal a 8. 141-128=13 por lo que ahora en la columna de la mitad derecha se busca el 13 y sus equivalencias son 1101 en binario y D en hexadecimal. Por lo tanto:

  $141_{10} = 10001101_2 = 8D_{16}$

- $C7_{16}$

La C_{16} corresponde a 192_{10} y 1100_2 y el 7_{16} a 7_{10} y a 0111_2.

$C7_{16} = 199_{10} = 11000111_2$

3.4.2 Tabla de *bits*

La tabla de *bit*s es simplemente una tabla que relaciona una columna con n a otra con 2^n-2. Es mejor hacer la tabla una vez al inicio del examen que calcular 2^n-2 para diferentes valores a lo largo del mismo. Claro que es todavía mejor, y preferible, aprenderse de memoria los valores de la tabla.

En el examen, se provee de una pizarra borrable así que, aprovechándola, es mejor hacer una tabla de 2^n simplemente comenzando con el número uno y duplicando el valor anterior en cada renglón y después restarle dos a cada número. Esto evitará alguna confusión.

3.4.3 Tabla de sub-redes

Como en el caso de la tabla de conversiones, resultaría bastante útil aprenderse absolutamente todas las sub-redes posibles para cada clase con todas las posibles máscaras. Por supuesto que esto es imposible, aún las combinaciones posibles en un solo octeto son demasiadas como para aprenderlas y manejarlas sin errores[1]. Sin embargo, generar la tabla condensada de todos los identificadores de sub-red en un octeto no es tan difícil y puede ser igual de útil.

La tabla tiene ocho columnas y como encabezado de cada una, un número en decimal que corresponde a incrementos de *bit* a *bit* sobre una máscara de sub-red. Del lado izquierdo se encuentran los números 8, 16 y 24 para cuando se requiera transformar de notación CIDR a decimal por octeto. Véase la tabla 3.10

8	9	10	11	12	13	14	15	16	2º octeto
16	17	18	19	20	21	22	23	24	3er octeto
24	25	26	27	28	29	30	31	32	4º octeto
	128	**192**	**224**	**240**	**248**	**252**	**254**	**255**	

Tabla 3.10 Encabezado de la tabla de sub-redes

De ese modo es fácil identificar una máscara de sub-red con la columna que se debe usar ya sea que se tenga en decimal como 255.255.248.0 ó en notación CIDR como /21.

En la columna central, la encabezada por la máscara 240 se tienen todos los identificadores de sub-red con esa máscara. Si la máscara llega al cuarto *bit* en un

[1] En el apéndice A se enlistan todas las posibles sub-redes que un octeto puede tener según sus diferentes máscaras de sub-red.

octeto, en ese octeto se tendrán para la parte de sub-red 4 *bits* y para la parte de *host* 4 *bits*, o sea que hay 16 combinaciones para cada sub-red. En otras palabras, los *Net ID*'s con esta máscara son 0, 16, 32, etc.

Una columna anterior, la 224 tendrá en ese octeto 5 *bits* para la parte de *host*, es decir que las sub-redes con esta máscara tendrán como *Net ID*'s en este octeto las 0, 32, 64, etc.

Cada columna, entonces, tendrá el doble de *hosts* que la de la derecha y la mitad de *hosts* que la de la izquierda y, consecuentemente, cada segundo *Net ID* de una columna lo será también de la columna a su izquierda, y también, todo *Net ID* de una columna también lo será de todas las columnas a su derecha, además de otros *Net ID*'s dependiendo de la columna que se trate.

Los *Net ID*'s en la columna 240 se encuentran sobre franjas en un tono gris obscuro que indican en qué columnas cada número es un *Net ID*.

En las columnas 248, 252, y 254 hay números entre paréntesis que indican la diferencia entre *Net ID* y *Net ID* en cada columna. Por lo tanto, para usar estas columnas, no es necesario calcular todos los *Net ID*'s sino tomar el *Net ID* de la franja más próxima y por las diferencias se sabrán los *Net ID*'s entre franja y franja.

Al conocer los *Net ID*'s de cada sub-red también se conoce que un número antes de cada *Net ID* es el *broadcast* de la sub-red anterior. Por ende, también se conoce el rango de IP's válidas en cada sub-red.

Hay en la tabla dos zonas con sombra en tono gris claro. La primera sub-red en cada red es la red cero y la última sub-red en cada red es una sub-red con solamente unos en la parte de sub-red. Por lo tanto, la primera y última sub-redes en una red no son válidas. Recordando que esta tabla es útil para analizar tan solo un octeto, el que un IP caiga en una de estas zonas no necesariamente lo hace inválido para asignarlo a un *host*, tan solo nos indica que dicho IP se compone exclusivamente de ceros (en la zona superior) o de unos (en la zona inferior) en el octeto que se examina. Esta información se tiene que considerar en conjunto con el resto del IP pero por si misma es muy útil para determinar la validez de un IP.

En las partes en donde la tabla tan sólo tiene el número cero o el 256 (que por cierto no debería ser parte de la tabla de no ser por este motivo) en sombra gris claro, eso significa que el sombreado cubre, respectivamente, la primera o la última sub-red disponible con la máscara correspondiente.

A continuación se presentan algunos ejercicios que ayudan a clarificar el uso de esta ayuda, pero definitivamente es necesario hacer muchos más para dominar su uso[2].

[2] Se pueden encontrar ejercicios de *subnetting* en la página de Cisco www.cisco.com entre otras.

Ejercicio 3.8

Para cada IP que se da a continuación, determinar el máximo de información a partir de las tablas de ayuda.

- 129.34.12.65/20

Dado que los 20 *bits* que marca la sub-máscara terminan en el tercer octeto, éste es el octeto que se analiza en la tabla. Se busca el cuadro que contenga el número 12 en la columna correspondiente a la máscara 20. Véase la tabla 3.11

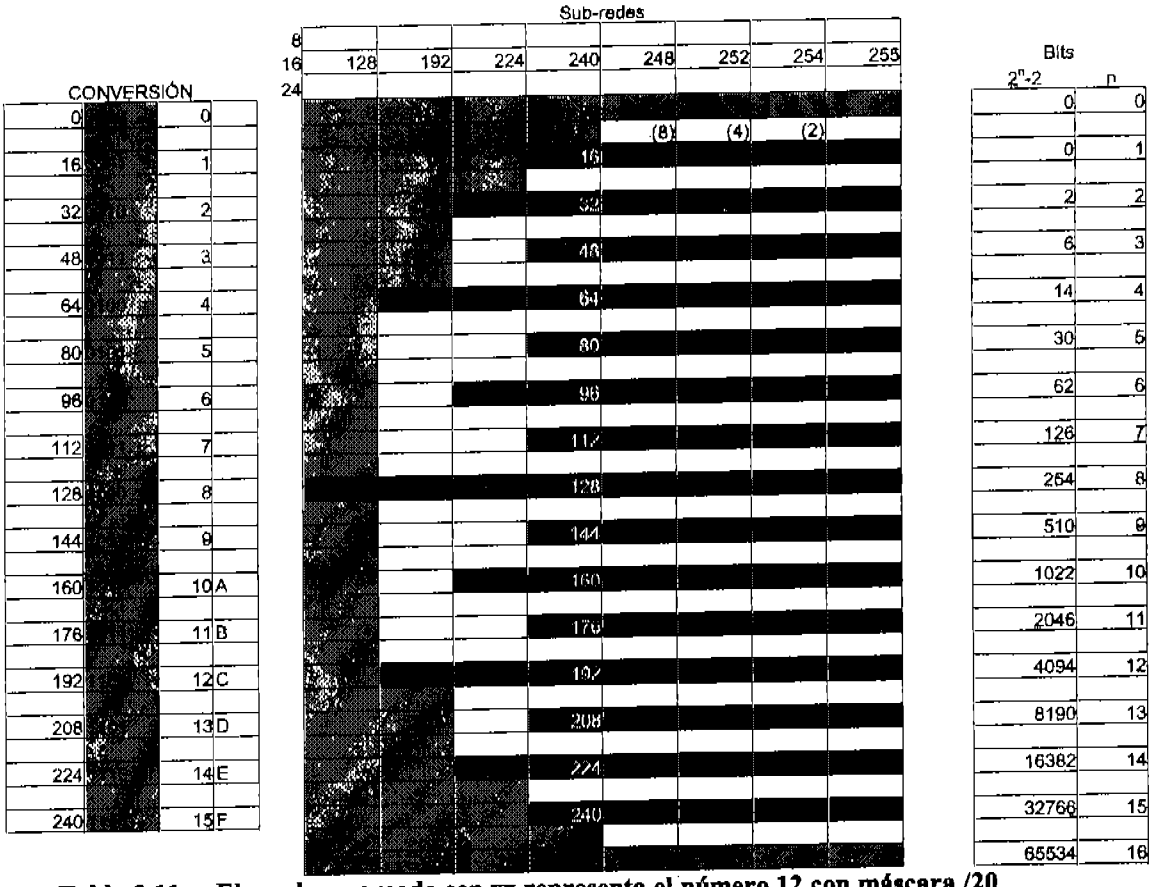


Tabla 3.11 El cuadro marcado con xx representa el número 12 con máscara /20

Como el 12 cae en la zona gris claro superior, se sabe que la parte de *Net ID* en el tercer octeto contiene solamente ceros. Como se trata de una red clase B. La parte de sub-red no abarca otro octeto además de la parte con ceros en el tercero. Por lo tanto este IP no es un IP válido.

- **145.16.200.38/27**

Se busca el 38 sobre la /27. Véase la tabla 3.12

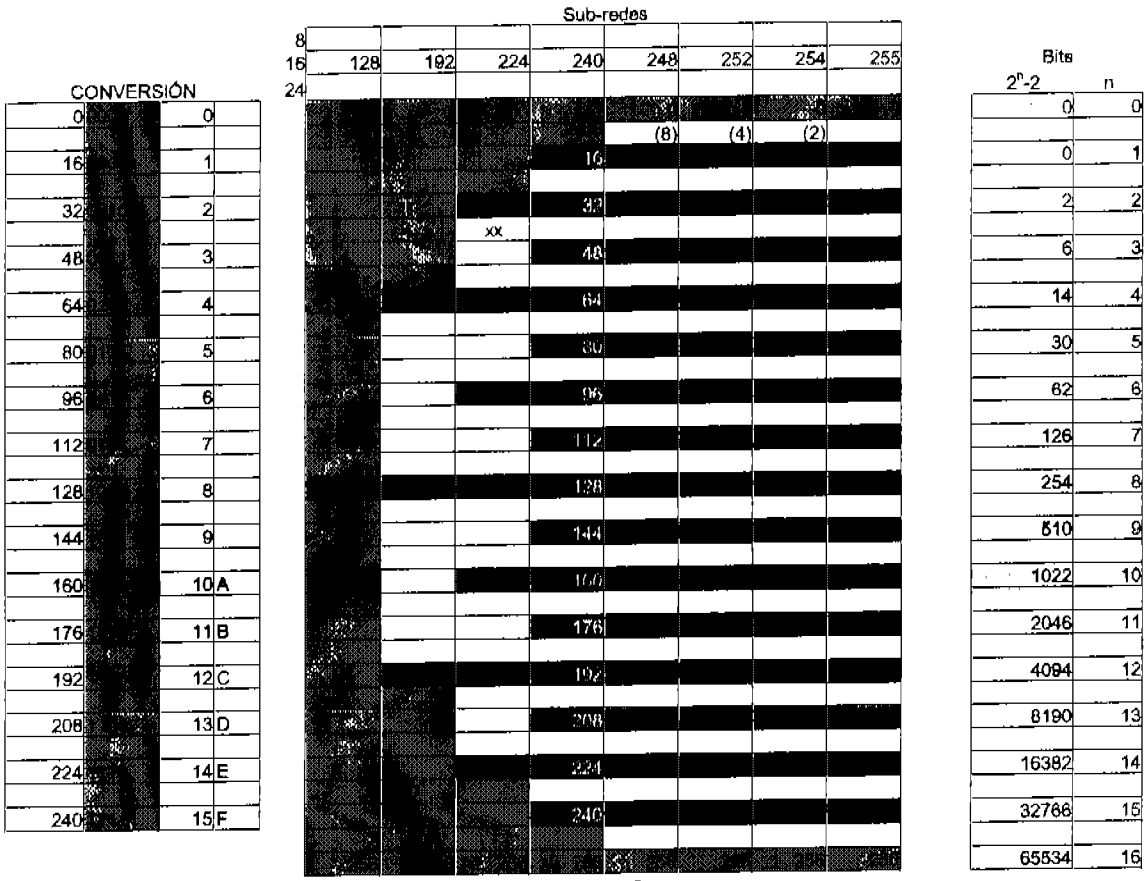


Tabla 3.12 El recuadro que se busca esta marcado con xx

De inmediato se sabe que la dirección es válida ya que cayó sobre un recuadro sin sombrear. El *Net ID* es la siguiente franja hacia arriba (32), el *broadcast* es uno antes del siguiente *Net ID* hacia abajo (64-1), hay tres *bits* en este octeto para la sub-red y 5 para el *host*.

Por lo tanto:

-*Net ID*: 145.16.200.32
-*Broadcast*: 145.16.200.63
-Rango de IP´s válidas en la sub-red: 145.16.200.33 a 145.16.200.62
-Sub-redes posibles con esta máscara: 8 *bits* del tercer octeto ya que se trata de una clase B y 3 del cuarto son 11 *bits* que en la tabla de *bits* corresponde a 2046
-*hosts* por sub-red: 5 *bits* en el cuarto octeto, utilizando la tabla de *bits* 5 corresponde a 30.

- 199.34.12.146/30

Se busca en la tabla 146 en /30 (Tabla 3.13)

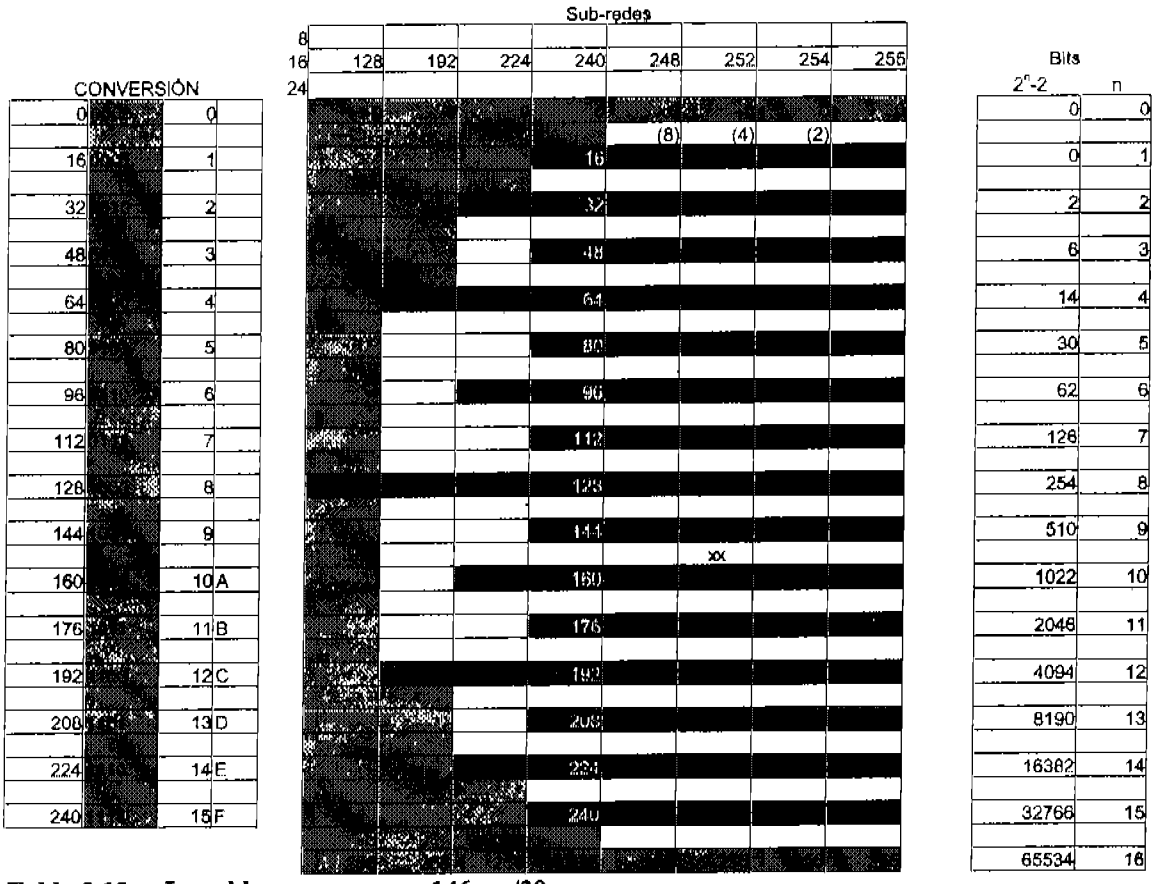


Tabla 3.13 La celda con xx marca 146 en /30

En este caso es importante recordar que hay más *Net ID*'s que los que las franjas muestran, pero se sabe que el 144 sí lo es y que el próximo se encuentra a cuatro IP's de distancia. Hay seis *bits* en la parte de sub-red y dos en la parte de *host*.

Por lo tanto,

-*Net ID*: 199.34.12.144
-*Broadcast*: 199.34.12.147 (148 es el próximo *Net ID*)
-Rango: 199.34.12.145 y 199.34.12.146
-Número de sub-redes: 62
-Número de *hosts*: 2

- 100.12.108.47/21

Se busca el 108 sobre la /21. (Tabla 3.14)

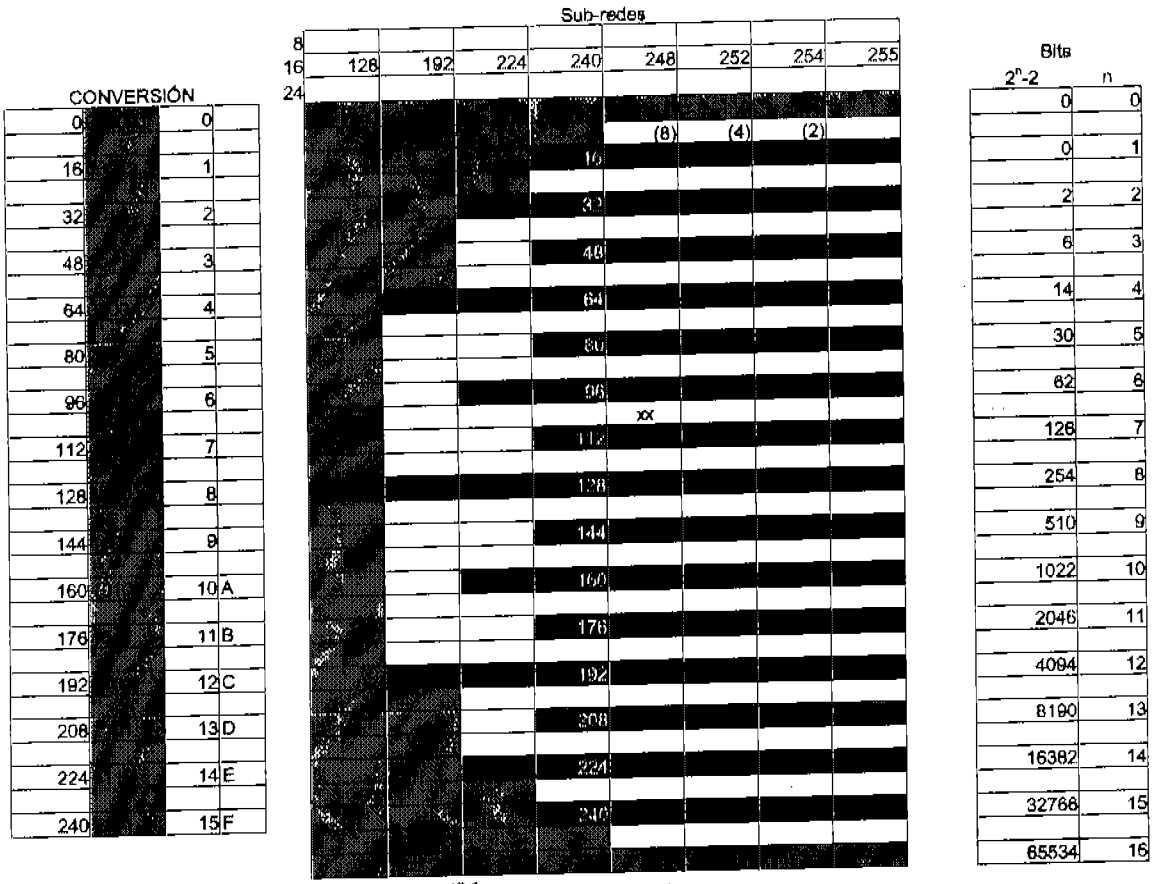


Tabla 3.14 La celda 108 sobre /21 se marca con xx

En este caso, los incrementos en los *Net ID*'s son de 8 en 8 así que entre las franjas 96 y 112 existe una más, la 104. Y, 108 se encuentra entre 104 y 112.

Por lo tanto,

Net ID: 100.12.104.0
Broadcast: 100.12.111.255
Rango: Desde 100.12.104.1 hasta 100.12.111.254
Número de sub-redes: (La parte de sub-red contiene 13 *bits*) 8190.
Número de *hosts* por sub-red: (la parte de *host* contiene 11 *bits*) 2046.

Se recomienda practicar con este método lo suficiente como para poder resolver un problema similar a los anteriores en aproximadamente 30 segundos y sin apuntar más que las respuestas.

3.5 VLSM (*Variable Length Subnet Masks*)

El método de asignación de máscaras de sub-red de longitud variable permite ahorrar espacio al asignar IP's en un ambiente ruteado. Tal como lo sugiere su nombre, el método de asignación de máscaras de longitud variable, consiste en asignar diferentes máscaras de sub-red a diferentes sub-redes dentro de la misma red. En la figura 3.11 se muestra un ejemplo de una red.

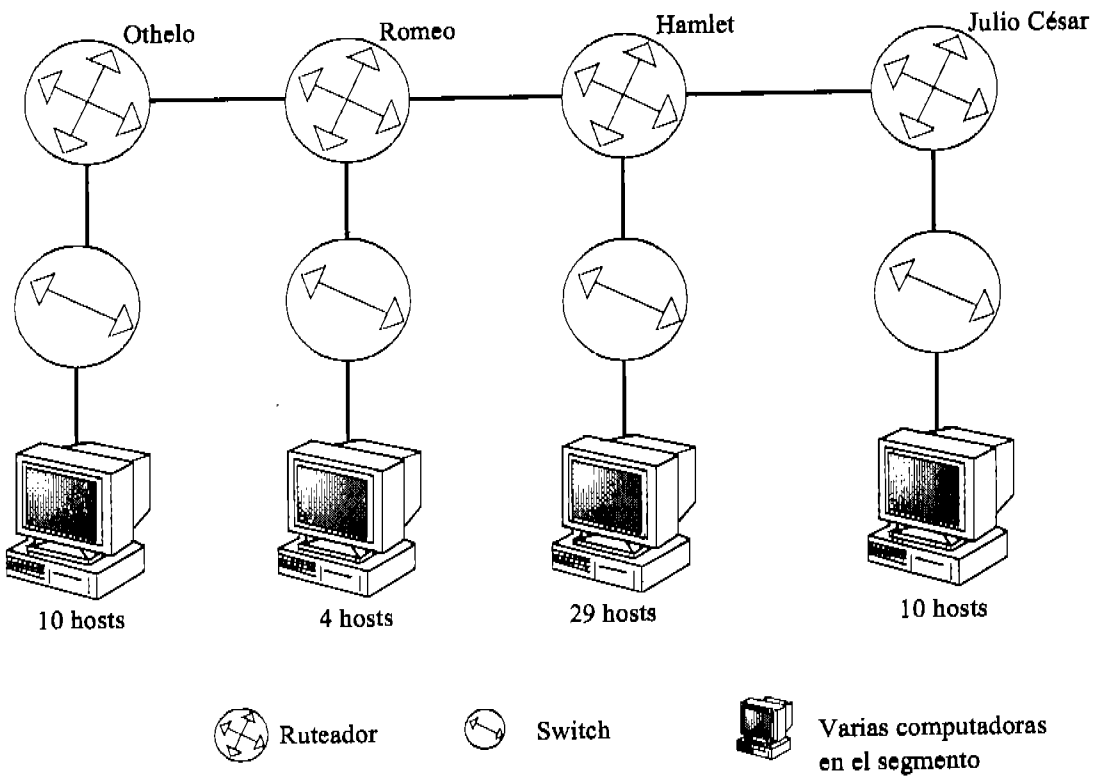


Figura 3.11 Red para el estudio de VLSM

3.5.1 Método *Classfull*

Considérese que la red de la figura 3.11 se implementa sobre la red 172.16.0.0 y que se requiere conectividad total entre las LANs. Si no se utiliza el método de VLSM, entonces se tiene que dividir la red por medio de la misma máscara de sub-red para cada una de las sub-redes. Al método en que se asignan máscaras de sub-red iguales a todas las sub-redes en una red se llama por clase o *classfull* (Protocolos como RIP o IGRP sólo funcionan en diseños *classfull.*)

En este primer escenario se tendría que escoger una máscara que albergue el número de IP's de la sub-red más grande. En este caso la LAN del ruteador Hamlet tiene 29 computadoras y una interfase del ruteador por lo que necesita asignar 30 IP's.

Para albergar 30 IP's se necesitan 5 *bits* por lo que la máscara que se debe utilizar para esta red es 255.255.255.224 ó /27.

Cada una de las sub-redes se asigna, utilizando la tabla de ayuda, como se muestra en la tabla 3.15

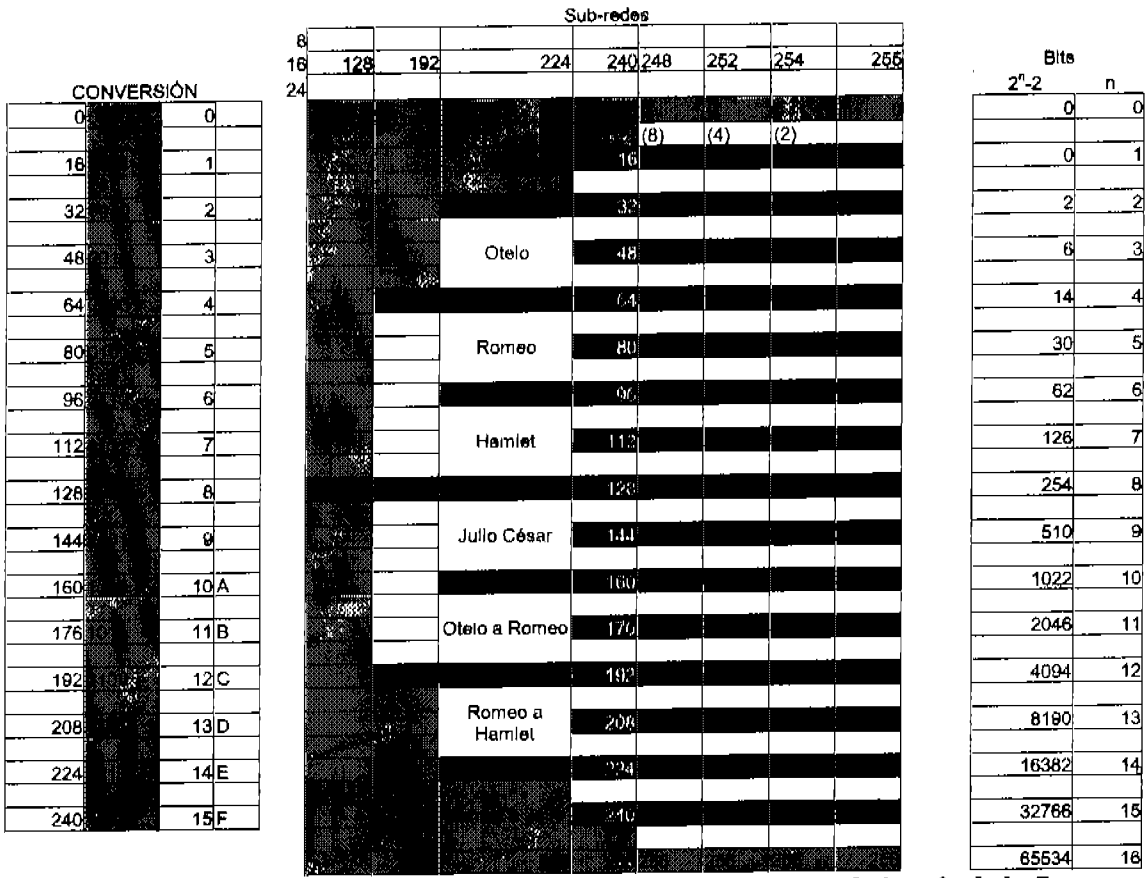


Tabla 3.15 Asignación por el método *classfull* de las sub-redes para el ejemplo de la figura 3.11

Nótese en la tabla 3.15 que la sub-red correspondiente a la liga que va de Hamlet a Julio César se encuentra en una zona gris claro, esto significa que en el octeto en que se está aplicando la máscara, la parte de sub-red se compone solamente de unos; pero en este caso no hay problema ya que la parte de sub-red se compone además de otro octeto entero el cual esta formado solamente por ceros, así que la parte de sub-red tiene ceros y unos por lo tanto es válida. (Esto no sucede en la primera sub-red de la red porque la parte de sub-red en el octeto analizado tiene sólo ceros y el octeto anterior, que también compone la parte de sub-red, también contiene sólo ceros. Así, la parte de sub-red tendría solamente ceros, lo cual no es válido.)

Las siete sub-redes del escenario tienen, respectivamente los siguientes identificadores de sub-red (*Net ID*'s): 172.16.0.32, 172.16.0.64, 172.16.0.96, 172.16.0.128, 172.16.0.160, 172.16.0.192 y 172.16.0.224. Véase la figura 3.12

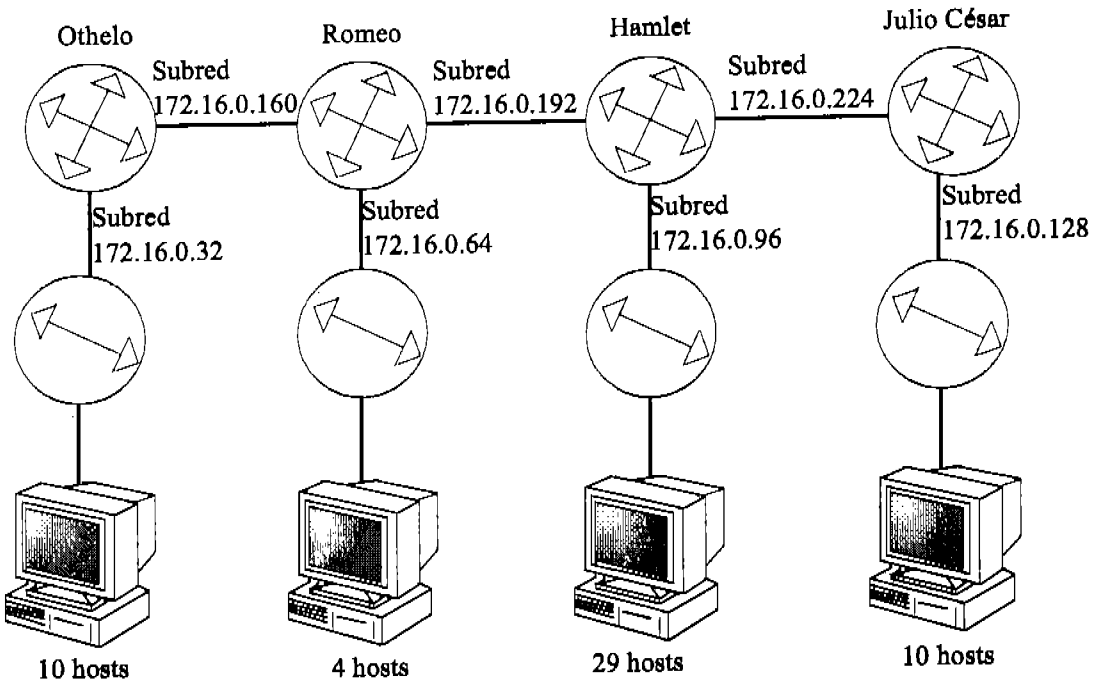


Figura 3.12 Una forma de asignar las sub-redes /27

Cada una de las sub-redes tiene un rango de 30 IP's asignables. Sin embargo, la única sub-red que requiere de 30 IP's es la 172.16.0.96, mientras que en resto de las sub-redes se desperdician IP's. De hecho, en las redes 172.16.0.160/27, 172.16.0.192/27 y la 172.16.0.224/27, solamente se necesitan dos IP's por sub-red (una para cada interfase de los ruteadores en esa sub-red), así que en tan sólo esas tres sub-redes se están desperdiciando 84 IP's.

3.5.2 Método VLSM

Si se asignan IP's al mismo escenario de la figura 3.11 pero ahora utilizando VLSM se podría hacer así:

La LAN de Otelo necesita 11 IP's. Una máscara de 4 *bit*s es suficiente para esta sub-red. Por ello se le asigna a la LAN de Otelo la máscara de sub-red /28.

La LAN de Romeo necesita 5 IP's. Estos se satisfacen con una máscara /29.

La LAN de Hamlet necesita 30 IP's, por lo que requiere una máscara /27.

La LAN de Julio César necesita 11 IP's, por lo tanto requiere una máscara /28.

Cada una de las sub-redes que enlazan dos ruteadores requieren solamente dos IP's por sub-red, por lo que tan solo se necesitan dos *bits* para los *hosts* en cada una de éstas sub-redes. La máscara adecuada para las sub-redes Otelo-Romeo, Romeo-Hamlet y Hamlet-Julio César es /30 en cada una.

Utilizando la tabla de ayuda, las sub-redes se pueden asignar como se muestra en la tabla 3.16.

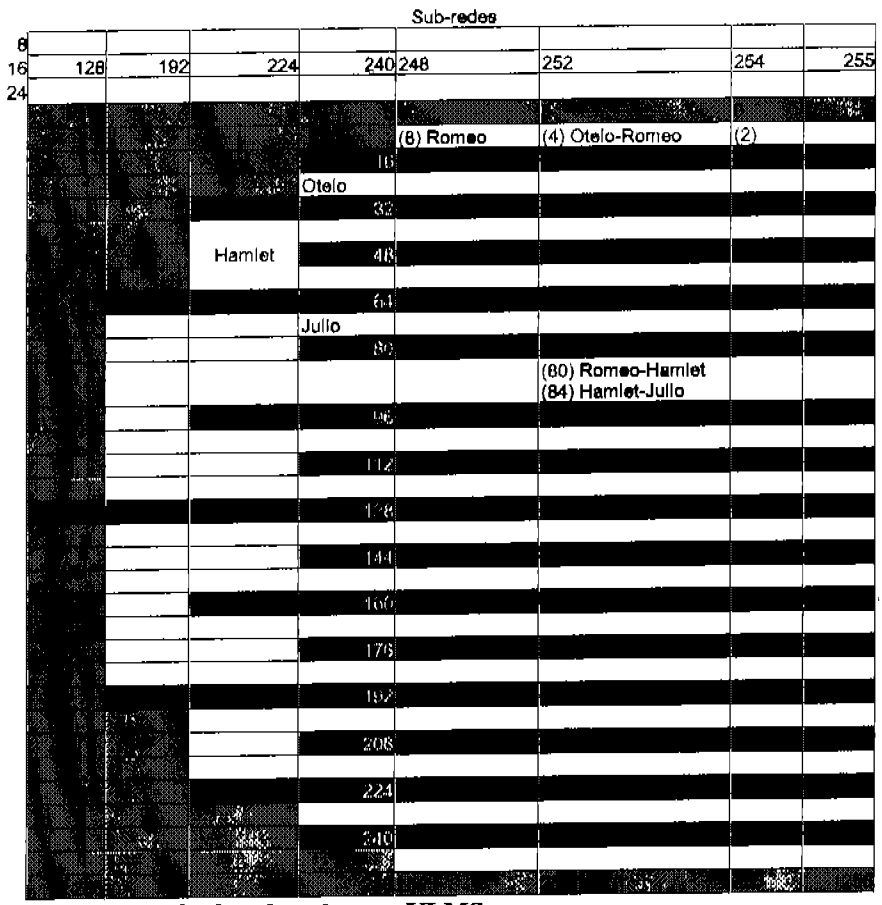


Tabla 3.16 Asignación de sub-redes con VLMS

El rango total para todas las sub-redes que se asignaron en la tabla 3.16 es desde 172.16.0.4 hasta 172.16.0.87. ¡Casi la cuarta parte de lo que se requirió con el método *classfull*!

Los *Net ID*'s en este escenario son: 172.16.0.4, 172.16.0.8, 172.16.0.16, 172.16.0.32, 172.16.0.64, 172.16.0.80 y 172.16.0.84.

El escenario con las IP's asignadas se muestra en la figura 3.13

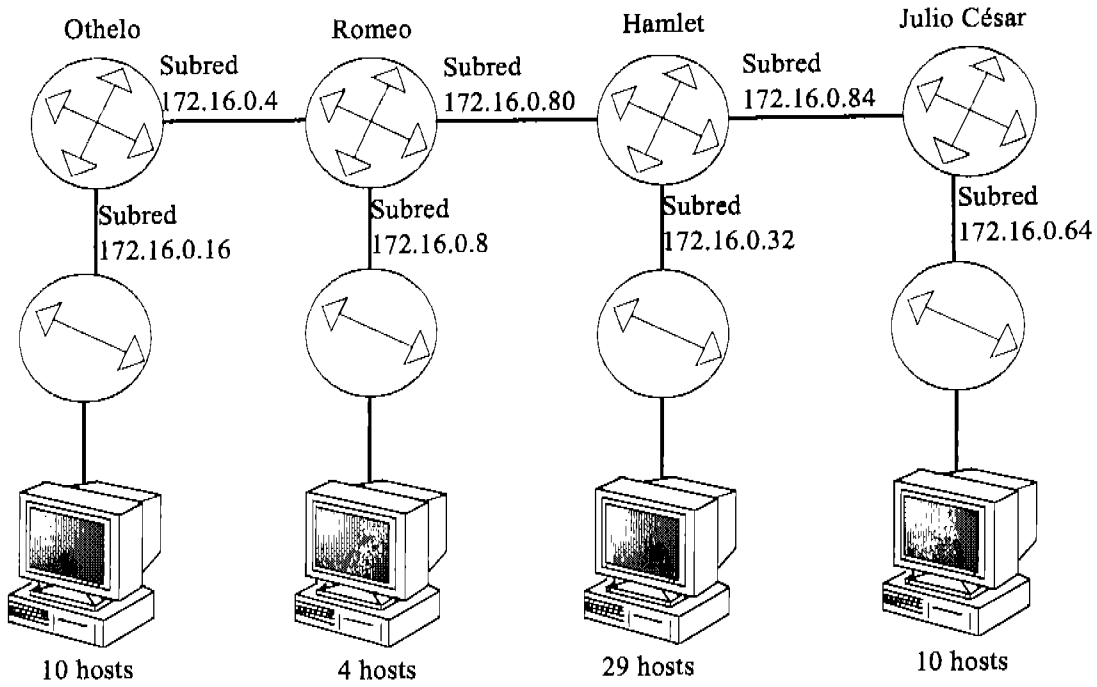


Figura 3.13 Asignación de IP´s utilizando VLSM

Ejercicio 3.9

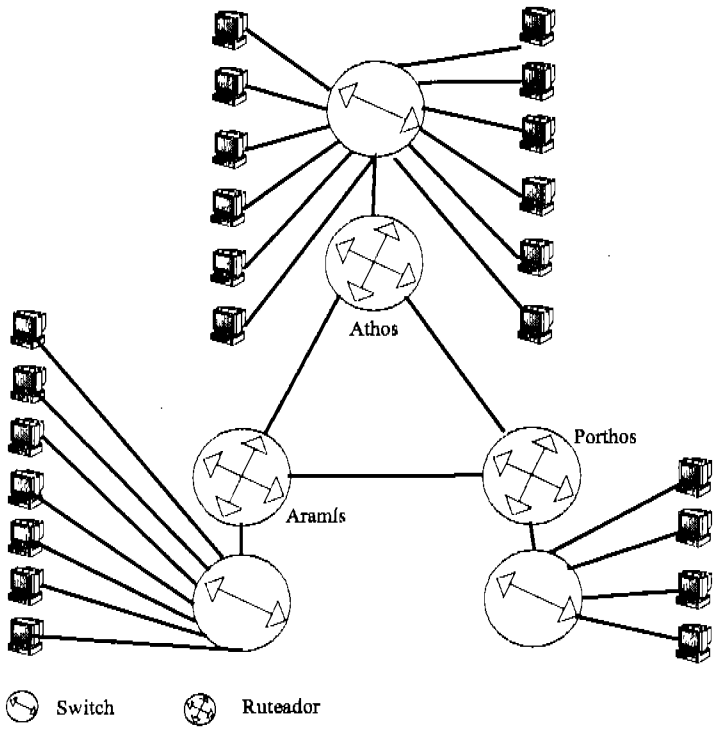


Figura 3.14 Escenario para el ejercicio 3.9

Asignar, utilizando VLSM, los IP's a las máquinas en la figura 3.14. Además, especificar los rangos de IP's disponibles, el *Net ID* y el *broadcast* para cada una de las sub-redes. Considérese que la red es 192.168.10.0.

En este escenario hay seis redes, tres de ellas son ligas WAN entre ruteadores que tan sólo necesitan dos direcciones IP, y las otras tres necesitan 13, 8 y 5 IP's.

Para la LAN de Athos, se necesitan 13 IP's (12 para computadoras, 1 para la interfase del ruteador.) Por lo que es conveniente utilizar una máscara /28.

La LAN de Porthos requiere de 5 IP's, por lo tanto su máscara es /29.

La LAN de Aramís necesita 8 IP's, así que su máscara de sub-red es /28.

Cada una de las WANs tiene una máscara /30.

Utilizando la tabla de ayuda de sub-redes se pueden asignar de la forma que se muestra en la tabla 3.17.

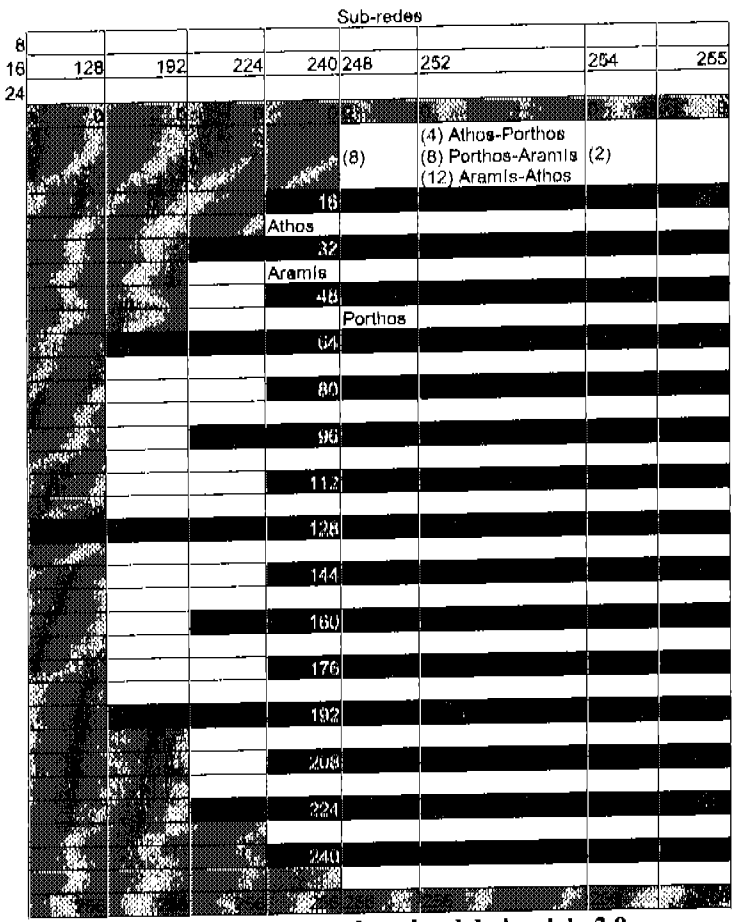


Tabla 3.17 Asignación de IP's para las sub-redes del ejercicio 3.9

Cada una de las sub-redes del ejercicio con su *Net ID*, su *broadcast* y el rango válido de IP's se enumeran a continuación.

Athos-Porthos
Net ID: 192.168.10.4
Broadcast: 192.168.10.7
Rango de IP's asignables: 192.168.10.5 y 192.168.10.6
IP's disponibles: 2

Porthos-Aramís
Net ID: 192.168.10.8
Broadcast: 192.168.10.11
Rango de IP's válidas: 192.168.10.9 y 192.168.10.10
IP's disponibles: 2

Aramís-Athos
Net ID: 192.168.10.12
Broadcast: 192.168.10.15
Rango de IP's válidas: 192.168.10.13 y 192.168.10.14
IP's disponibles: 2

Athos
Net ID: 192.168.10.16
Broadcast: 192.168.10.31
Rango de IP's válidas: 192.168.10.17 al 192.168.10.30
IP's disponibles: 14

Aramís
Net ID: 192.168.10.32
Broadcast: 192.168.10.47
Rango de IP's válidas: 192.168.10.33 al 192.168.10.46
IP's disponibles: 14

Porthos
Net ID: 192.168.10.48
Broadcast: 192.168.10.55
Rango de IP's válidas: 192.168.10.49 al 192.168.10.54
IP's disponibles: 6

Al asignar las direcciones en el escenario, se sigue una norma no escrita en la que a las interfases de los ruteadores se les trata siempre de asignar la primera dirección disponible en el segmento en el que se encuentra. Esto, por supuesto, no tiene implicaciones técnicas. Sin embargo, es una práctica muy recomendable.

En la figura 3.15 se muestra la asignación de las IP's a los dispositivos del escenario de acuerdo a lo calculado.

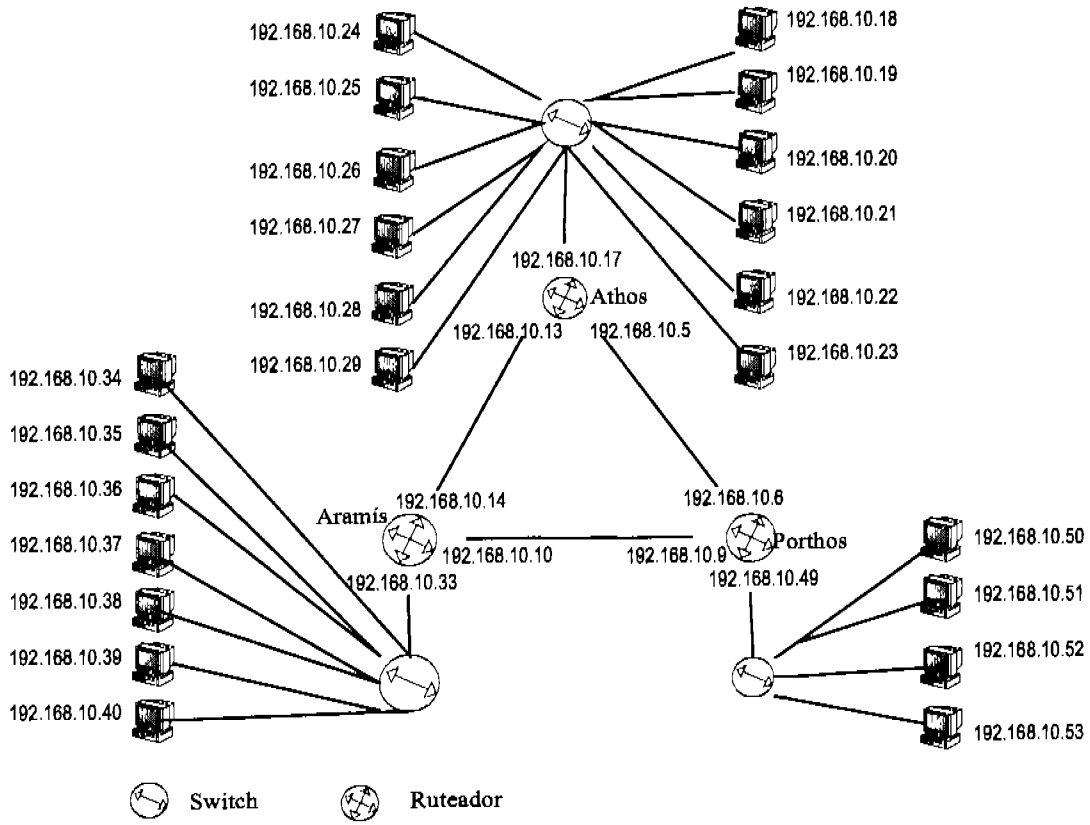


Figura 3.15 IP's asignadas con VLSM para el ejercicio 3.9

En los siguientes capítulos se utilizan escenarios ya calculados. Se recomienda en todos los casos practicar la asignación de IP's y el cálculo de sub-redes en dichos escenarios. Además de los que se puedan encontrar en la red. Cisco da bastantes ligas en Internet de sitios en donde se pueden encontrar ejercicios, algunos de estos sitios son gratuitos.[3]

[3] www.cisco.com

Capítulo 4

Comandos Básicos del IOS

4.1 Introducción

En este capítulo se presentan aspectos básicos en el manejo de un ruteador Cisco. Al igual que las computadoras de escritorio, los ruteadores necesitan un sistema operativo, en el caso de Cisco, este es el IOS (*Internetwork Operating System.*)

Existen dos maneras de configurar el IOS de un ruteador: a través del ayudante de configuración (*Setup*) y de la línea de comandos, CLI (*Command Line Interface.*)

Tanto en este capítulo como en los siguientes se muestran las respuestas de un ruteador a diferentes comandos y configuraciones. Estas configuraciones pueden variar según el modelo de ruteador que se utilice, sin embargo, dichas variaciones serán mínimas gracias a Cisco Fusion. Cisco Fusion permite que todos los ruteadores diseñados por Cisco corran bajo el mismo sistema operativo IOS.

Aunque los ejercicios presentados en este manual ilustran de manera general los conceptos discutidos, por motivos de espacio no se muestran todas las variaciones posibles en cada caso, por lo que es muy recomendable que se busque practicar el uso de los comandos utilizando un ruteador real o un simulador de ruteo.

Aunque es posible comprar un ruteador usado en buenas condiciones por un costo bastante bajo, es preferible buscar un simulador de ruteo, ya que en el simulador se tendrán en pantalla las respuestas del ruteador tal como estas se verían con un ruteador real, pero además, en el simulador es posible utilizar varios ruteadores y configurarlos para formar una red en la que se puedan poner en práctica conceptos que en un solo ruteador no sería posible.

Hay varios simuladores en el mercado, algunos de ellos son gratuitos y otros más ofrecen periodos gratuitos de prueba. Personalmente me agradan los simuladores de Routersim y de Boson, que son muy completos y tienen costos accesibles. Pero a final de cuentas, es una buena idea comenzar con las versiones de evaluación y decidir cual se adecua mejor al estilo particular.

4.2 Interacción con el Ruteador Cisco

4.2.1 Estructura de los ruteadores Cisco

Hay una gran variedad de modelos de ruteadores Cisco, desde ruteadores muy pequeños con pocas interfases, hasta ruteadores que soportan decenas de interfases. Algunos modelos cuentan con un número fijo de interfases, mientras que otros cuentan con un sistema modular en el que es posible insertar diferentes interfases en ranuras (*slots*) dispuestas para ese propósito y que hacen a estos ruteadores muy versátiles. La tabla 4.1 muestra las interfases que tienen algunos de los ruteadores más utilizados.

Interfases en Algunos de los Ruteadores mas comunes								
Serie	Modelo	Numero de Interfases					Modulos WAN	
		Ethernet	Serial	Bri	Token	Fast E.	Num.	Cada Modulo puede tener una de las slg. opciones
800								
	801	1		1				
	803	1		1				
	804	1		1				
	805	1	1					
	808	2						
1000								
	1003	1		1				
	1004	1		1				
	1005	1	1					
1600								
	1601	1	1				1	(1 Serial) (1 Bri)
	1602	1						(1 Serial) (1 Bri)
	1603	1		1				(1 Serial) (1 Bri)
	1604	1		1				(1 Serial) (1 Bri)
	1605	2						(1 Serial) (1 Bri)
1700								
	1710	1			1	1		
	1720				1	1	2	(1 Serial) (2 serial) (1 Bri) (1 Ethernet)
	1721				1	1	2	(1 Serial) (2 serial) (1 Bri) (1 Ethernet)
	1750				1	1	2	(1 Serial) (2 serial) (1 Bri) (1 Ethernet)
	1751				1	1	2	(1 Serial) (2 serial) (1 Bri) (1 Ethernet)
	1760				1	1	2	(1 Serial) (2 serial) (1 Bri) (1 Ethernet)
2500								
	2501	1	2					
	2502		2		1			
	2503	1	2	1				
	2504		2	1	1			
	2505	1	2					
	2507	1	2					
	2509	1	8					
	2513	1	2		1			
	2514	2	2					
	2515		2		2			
	2516	1	2	1				
	2520	1	4	1				
	2521		4	1	1			
	2522	1	10	1				
	2523		10	1	1			

Tabla 4.1 Interfases en algunos ruteadores

Algunos de los Ruteadores mas comunes								
Serie	Modelo	Numero de Interfases					Modulos WAN	
		Ethernet	Serial	Bri	Token	Fast E.	Num.	Cada Modulo puede tener una de las sig. Opciones
2600								
	2610	1					2	(1 Serial) (2 serial) (1 Bri)
	2611	1					2	(1 Serial) (2 serial) (1 Bri)
	2620					1	2	(1 Serial) (2 serial) (1 Bri)
	2621					2	2	(1 Serial) (2 serial) (1 Bri)
3600								
	3620						2	(1E) (4E) (1E, 1S) (2E, 1S) (1F) (1F, 1B) (1F, 2B) (4S) (1B)
	3640						4	(1E) (4E) (1E, 1S) (2E, 1S) (1F) (1F, 1B) (1F, 2B) (4S) (1B)
4500								
	4500						3	(2E) (4E) (1F) (2S) (4S) (1B)

Tabla 4.1(continuación) Interfases en algunos ruteadores

Las figuras 4.1 y 4.2 muestran de manera esquemática un ruteador 2501 y uno 2600.

Figura 4.1 Esquema de un ruteador 2501

Figura 4.2 Esquema de un ruteador 2600

Los ruteadores Cisco cuentan con tres tipos principales de memoria: la memoria Flash, la memoria NVRAM, y la memoria RAM.

La memoria Flash, es una memoria tipo EEPROM en la cual se almacena el IOS. En la memoria NVRAM (*Non Volatile* RAM) se guarda la configuración con la que el ruteador se inicializará al arrancar. Y la memoria RAM es la memoria en la que radica la configuración que el usuario maneja al realizar cambios al ruteador.

Cuando un ruteador Cisco arranca, se realiza un autoreconocimiento llamado POST (*Power On Self Test.*) Si no hay problemas en el ruteador al efectuar el POST, el ruteador busca el IOS en la memoria Flash y lo carga. A continuación el IOS busca en la memoria NVRAM la configuración de arranque con la que debe inicializar el ruteador. Esta configuración se llama *startup-config*. La configuración de arranque se carga también en RAM y a esta configuración se le llama *running-config*.

En caso de que el ruteador no encuentre una configuración válida en la NVRAM iniciará el "ayudante" para la inicialización asistida (*Setup Mode.*) El setup mode se discute más adelante en este capítulo.

Al trabajar en un ruteador, los cambios se realizan en RAM (*running-config*), y aunque se ponen en efecto de inmediato, éstos no se guardan automáticamente en la memoria NVRAM (*startup-config.*) Para que la siguiente vez que se encienda el ruteador éste se inicialice con los cambios hechos en RAM, es necesario copiar la RAM a NVRAM *(running-config* a la *startup-config.)*

4.2.2 Conexión a un ruteador Cisco

Hay tres formas para establecer una sesión en un ruteador: a través de la consola, a través del puerto auxiliar y por medio de Telnet.

Para establecer una sesión por medio de la consola del ruteador, se utiliza un cable rolled[1] para conectar la consola al puerto de comunicaciones de la computadora a conectar. La conexión se establece por medio de HyperTerminal. Véase la figura 4.3

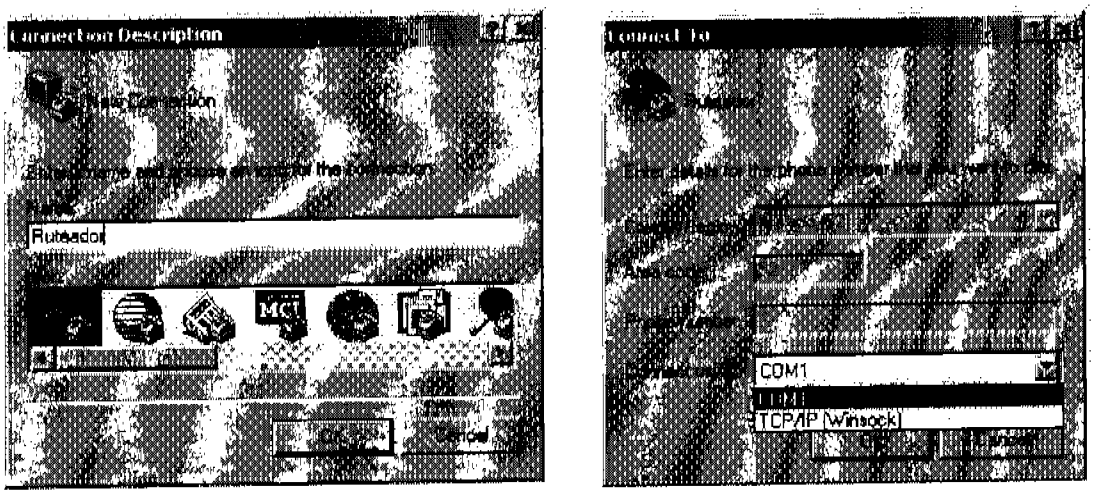


Figura 4.3 Después de iniciar la aplicación Hyperterminal, se establece un nombre para la conexión y se selecciona que la conexión se realizará por uno de los puertos de comunicaciones del equipo.

[1] El cable rolled se menciona en la página 46.

En las propiedades de la conexión del puerto COM que se utiliza, se establece una velocidad de transmisión de 9600 *bit*s por segundo y el control de flujo se cambia a "ninguno". Es importante recordar estos parámetros porque no son los preestablecidos por la conexión y hay que cambiarlos.

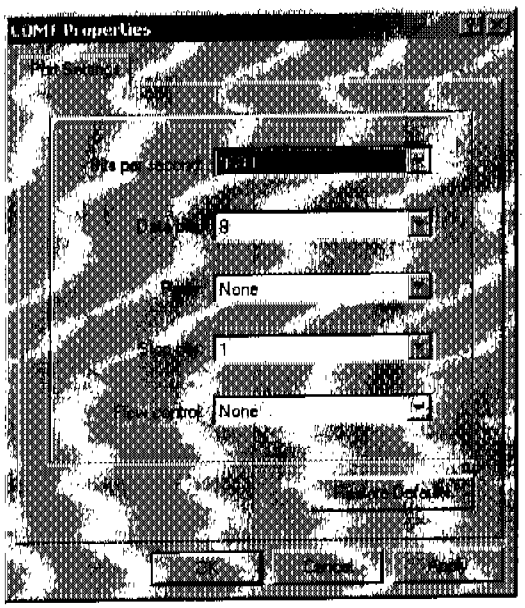


Figura 4.4 Las propiedades de la conexión deben ser las mostradas en la figura.

Al aceptar estos parámetros se inicia la conexión por medio de la consola con el ruteador.

La conexión al ruteador por medio del puerto auxiliar funciona tal como la conexión por medio de la consola, con la diferencia de que la conexión por medio del puerto auxiliar permite además, conectarse al ruteador a través de un módem, lo que hace posible utilizar la red telefónica para configurar remotamente un ruteador.

La conexión por medio de Telnet también permite accesar al ruteador de manera remota pero en este caso, esto se logra desde la red computacional. Telnet permite emular al ruteador en una PC remota tal como si se estuviera frente a él.

4.2.3 Modo de configuración guiada

Cuando un ruteador Cisco arranca carga el IOS y después busca una configuración válida para inicializarse con parámetros tales como IP's, listas de acceso, protocolos, etc. Sin embargo, esta configuración no siempre está disponible. Cuando el IOS no encuentra una configuración válida de inicio, el ruteador entra automáticamente al modo de configuración guiada (*setup mode.*) Otra manera de entrar a este modo es escribiendo el comando setup desde la línea de comandos en el modo privilegiado

(el modo privilegiado se discute en la sección 4.2 en el subtema "Niveles de Acceso al Ruteador".)

A continuación se muestra la salida de un ruteador de la serie 2500 al arrancar[2]:

System Bootstrap, Version 11.0(10c)XB1, PLATFORM SPECIFIC RELEASE SOFTWARE (fc1)

Copyright (c) 1986-1997 by cisco Systems
2500 processor with 4096 Kbytes of main memory

Notice: NVRAM invalid, possibly due to write erase.

F3: 3412856+84828+215720 at 0x3000060

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco Internetwork Operating System Software
IOS (tm) 3000 Software (IGS-I-L), Version 11.0(7), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1996 by cisco Systems, Inc.
Compiled Thu 28-Mar-96 18:27 by dschwart
Image text-base: 0x0301D924, data-base: 0x00001000

cisco 2511 (68030) processor (revision D) with 4096K/2048K bytes of memory.
Processor board ID 01913096, with hardware revision 00000000
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
Primary Rate ISDN software, Version 1.0.
1 Ethernet/IEEE 802.3 interface.
2 Serial network interfaces.

---

[2] Nota: la respuesta del ruteador se identifica con este tipo de letra y las entradas de usuario dadas en línea de comandos se identifican **con este tipo de letra.**

16 terminal lines.
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read ONLY)

Notice: NVRAM invalid, possibly due to write erase.
--- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Would you like to enter the initial configuration dialog? [yes]: **[Enter]**
At any point you may enter a question mark '?' for help
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Would you like to enter the initial configuration dialog? [yes]: **[Enter]**

First, would you like to see the current interface summary? [yes]: **[Enter]**

Any interface listed with OK? value "NO" does not have a valid configuration

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0	unassigned	NO	not set	up	down
Serial0	unassigned	NO	not set		
Serial1	unassigned	NO	not set	down	down

Configuring global parameters:

Enter host name [Router]: **cancun**

The enable secret is a one-way cryptographic secret used
instead of the enable password when it exists.

Enter enable secret: **secreto**
The enable password is used when there is no enable secret
and when using older software and some boot images.

Enter enable password: **habilitar**
Enter virtual terminal password: **telnet**
Configure SNMP Network Management? [yes]: **n**
Configure IP? [yes]: **[Enter]**
Configure IGRP routing? [yes]: **n**
Configure RIP routing? [no]: **n**

```
  Configure Async lines? [yes]: n

Configuring interface parameters:

Configuring interface Ethernet0:
  Is this interface in use? [yes]: [ Enter ]
  Configure IP on this interface? [yes]: [ Enter ]
    IP address for this interface: 172.16.1.1
    Number of bits in subnet field [0]: [ Enter ]
    Class B network is 172.16.0.0, 0 subnet bits; mask is 255.255.0.0

Configuring interface Serial0:
  Is this interface in use? [yes]: [ Enter ]
  Configure IP on this
  Configure IP unnumbered on this interface? [no]: [ Enter ]
    IP address for this interface: 172.17.1.1
    Number of bits in subnet field [0]: [ Enter ]
    Class B network is 172.17.0.0, 0 subnet bits; mask is 255.255.0.0

Configuring interface Serial1:
  Is this interface in use? [yes]: n

The following configuration command script was created:

hostname cancun
enable secret 5 $1$s64f$QN0xAfT04bTJ.Qeg8ezFA0
enable password habilitar
line vty 0 4
password telnet
no snmp-server
!
ip routing
!
interface Ethernet0
ip address 172.16.1.1 255.255.0.0
!
interface Serial0
ip address 172.17.1.1 255.255.0.0
!
interface Serial1
shutdown
no ip address
!
```

```
end

Use this configuration? [yes/no]:
```

En este punto en el estudio no es importante entender lo que cada renglón significa, sino, ver un ejemplo de lo que se puede configurar por medio del modo de configuración guiada.

Nótese que al buscar una configuración valida, no se encuentra ninguna y por lo tanto el sistema entra al modo asistido (System Configuration Dialog.) Hay dos formas de salir del diálogo de configuración, la primera es: en cualquier momento de la configuración, presionar **Ctrl + C**, lo que provocará que se aborte la secuencia de configuración y no se guarden los cambios realizados hasta el momento. La segunda forma es contestando la pregunta al final de la configuración. Por supuesto que si se responde con "no", no se guarda la configuración y el resultado es prácticamente el mismo de interrumpir la secuencia de configuración con **Ctrl + C**.

Varias preguntas del modo de configuración asistido incluyen una respuesta por omisión entre corchetes [ ], la cual toma el ruteador con sólo presionar **Enter**.

El objetivo del modo de configuración guiado es permitir a un usuario no experimentado, programar de manera muy básica un ruteador para que éste tenga, también de forma muy básica, la conectividad necesaria para direccionar los paquetes de la red en la que se encuentre.

4.3 Comandos en Línea

A pesar de la sencillez para configurar un ruteador por medio del modo de configuración guiado, éste no es el mejor método para hacerlo. El mejor método para configurar un ruteador Cisco es a través de la línea de comandos, CLI (*Command Line Interface.*) Para configurar, a través de la línea de comandos, un ruteador que no cuenta con una configuración startup-config válida tan solo hay que rechazar entrar al modo guiado.

```
Notice: NVRAM invalid, possibly due to write erase.
        --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help
Default settings are in square brackets '[ ]'.
Would you like to enter the initial configuration dialog? [yes]: n

Would you like to terminate autoinstall? [yes]: [ Enter ]

Press RETURN to get started!
```

4.3.1 Niveles de acceso al ruteador

Hay varios niveles de acceso al ruteador, cada uno se identifica por un diferente prompt o indicador, en el siguiente ejemplo se muestra el cambio del indicador para algunos de éstos niveles:

```
Router con0 is now available

Press RETURN to get started. [ Enter ]

Router>
```

Después de iniciar el ruteador en modo CLI, el primer indicador, Router>, muestra que se está en el modo usuario, (*user exec mode*) en este modo se pueden utilizar varios comandos que principalmente tienen que ver con el monitoreo de la actividad del ruteador. El siguiente indicador se obtiene al teclear el comando **enable**, este indicador, router#, muestra que se ésta en el modo de usuario privilegiado. Desde este prompt es posible monitorear la actividad y configuración del ruteador y también cambiarlas. La mayoría de los comandos del IOS de Cisco existen tan sólo en un sentido y para hacer lo contrario se utilizan precedidos de la palabra "**no**". El comando **enable** es una de las pocas excepciones a esto, al existir el comando **disable**, el cual cambia el ruteador de modo de usuario privilegiado a usuario normal.

```
Router>enable
Router#
Router#disable
Router>
```

Al introducir el comando **configure** se tiene acceso al modo de configuración del ruteador, la configuración se puede realizar por medio de comandos en línea introducidos al momento en la terminal, por medio de un archivo previamente introducido a la memoria o por medio de un servidor TFTP en la red. La opción por omisión es "terminal".

```
Router>enable
Router#configure
Configuring from terminal, memory, or network [terminal]? [ Enter ]
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#^Z
Router#
```

Para salir por completo del modo de configuración, se puede presionar la secuencia **Ctrl + Z**. Otra forma de iniciar el modo de configuración es especificando la forma por la cual se introducirá la información.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

La única manera de llegar al modo de configuración es a través del modo de usuario privilegiado.

```
Router>configure terminal
        ^
% Invalid input detected at '^' marker.

Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

Nótese que el ruteador indica con una pequeña marca (^) el lugar exacto en donde desconoce el comando introducido. Una vez aceptado el comando **configure terminal** el indicador cambia para mostrar el modo en que ahora se encuentra el ruteador.

Tan sólo para mostrar otros modos de operación del ruteador y sus indicadores asociados se muestra el siguiente ejemplo. Por el momento no es importarte conocer lo que cada indicador significa:

```
Router>
```

Modo usuario

```
Router>enable
Router#
```

Modo de usuario privilegiado

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

Modo de configuración global

```
Router(config)#line console 0
```

```
Router(config-line)#
```

Modo de configuración de línea de acceso (en este ejemplo la línea de acceso es la consola del ruteador)

```
Router(config-line)#exit
Router(config)#
```

La palabra **exit** permite salir de un nivel al nivel anterior.

```
Router(config)#interface serial 0
Router(config-if)#
```

Modo de configuración de interfases (interfase serial 0 en este caso)

```
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#
```

Modo de configuración de protocolos de ruteo (RIP en el ejemplo)

```
Router(config-router)#exit
Router(config)#interface serial 0.1
Router(config-subif)#
```

Modo de configuracion de subinterfases (serial 0.1 en el ejemplo)

```
Router(config-subif)#exit
Router(config)#exit
Router#
```

4.3.2 Ayuda ínter-construida

En un principio, podría parecer que para utilizar el CLI del IOS de un ruteador es necesario conocer muchos comandos y palabras reservadas, sin embargo, esto no necesariamente es cierto gracias a que el IOS de Cisco cuenta con ayuda ínter construida.

Para hacer uso de la ayuda ínter construida tan sólo hay que presionar la tecla " ? " . al hacerlo, el ruteador da una lista de los posibles comandos desde el modo en que se encuentre:

```
Router>?
Exec commands:
```

```
connect          Open a terminal connection
disable          Turn off privileged commands
disconnect       Disconnect an existing network connection
enable           Turn on privileged commands
exit             Exit from the EXEC
help             Description of the interactive help system
lock             Lock the terminal
login            Log in as a particular user
logout           Exit from the EXEC
```

(Por motivos de espacio, la respuesta del ruteador se corta)

```
Router(config-line)#?
Line configuration commands:
 absolute-timeout    Set absolute timeout for line disconnection
 access-class        Filter connections based on an IP access list
 activation-character  Define the activation character
 autocommand         Automatically execute an EXEC command
 autohangu       Automatically hangup when last connection closes
 autoselect          Set line to autoselect
 data-character-bits  Size of characters being handled
 databits            Set number of data bits per character
 disconnect-character  Define the disconnect character
 dispatch-character  Define the dispatch character
 dispatch-machine    Reference a TCP dispatch state machine
 dispatch-timeout    Set the dispatch timer
 editing           Enable command line editing
 escape-characte     Change the current line's escape character
 exec              Start an EXEC process
 exec-banner         Enable the display of the EXEC banner
 exec-character-bits  Size of characters to the command exec
 exec-timeout        Set the EXEC timeout
 exit              Exit from line configuration mode
 flowcontrol         Set the flow control
 full-help         Provide help to unprivileged user
--More--
```

(Aquí se corta la respuesta)

Nótese que la respuesta del ruteador al mismo caracter de entrada es diferente, dependiendo del indicador en el que se introduzca. Aún más, el signo de interrogación se puede introducir después de una o varias palabras y el ruteador dará las opciones para la siguiente palabra del comando.

```
Router#?
Exec commands:
  bfe              For manual emergency modes setting
  clear            Reset functions
  clock            Manage the system clock
  configure        Enter configuration mode
  connect          Open a terminal connection
  copy             Copy configuration or image data
  debug            Debugging functions (see also 'undebug')
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  enable           Turn on privileged commands
  erase            Erase flash or configuration memory
  exit             Exit from the EXEC
```

(Respuesta cortada.)

```
Router#configure ?
  memory           Configure from NV memory
  network          Configure from a TFTP network host
  overwrite-network  Overwrite NV memory from TFTP network host
  terminal         Configure from the terminal
  <cr>

Router#configure terminal ?
  <cr>
```

La opción **<cr>** significa "*carry return*" (simplemente *Enter*.)

```
Router#configure terminal [ Enter ]
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

Después de dar las opciones disponibles en cada caso, el ruteador vuelve a poner el indicador correspondiente y las palabras del comando que se han introducido hasta el momento para que el usuario tan sólo tenga que poner la siguiente palabra.

También es posible utilizar el signo de interrogación para desplegar opciones de comandos que comiencen de cierta manera. Por ejemplo, si en modo de configuración global se quiere tener un listado de los comandos disponibles que comiencen con la letra "c", se puede hacer lo siguiente:

```
Router(config)#c?
cdp  chat-script  clock  config-register
```

```
Router(config)#c
```

Otra forma de ayuda que ofrece el ruteador Cisco es la tecla **[Tab]**. Esta tecla hace que el ruteador complete la palabra que se comienza a escribir en la línea de comandos, el único requisito es que tan sólo exista un comando que inicie con la porción escrita.

```
Router#conf[ Tab ]
Router#configure t[ Tab ]
Router#configure terminal
```

De hecho, si no hay ambigüedades, no es necesario escribir las palabras completas en los comandos para que el ruteador los entienda.

```
Router#con[ Enter ]
% Ambiguous command: "con"
Router#con?
configure  connect
```

Como se puede ver, hay dos comandos disponibles desde el modo privilegiado que comienzan con las letras "con" por lo que al poner **con + [Enter]** el ruteador no sabe a que comando se refiere el usuario y responde con la leyenda "*Ambiguous command*".

```
Router#conf[ Enter ]
Configuring from terminal, memory, or network [terminal]?t[ Enter ]
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

En este caso, el único comando que comienza con "conf" es **configure** por lo tanto el ruteador lo reconoce y lo ejecuta. Al igual que la letra "t" cuando se pide especificar la forma de configuración.

4.3.3 Nombres

Una característica muy útil cuando se trabaja con varios ruteadores, es la facultad de nombrarlos. A pesar de que el nombre que se le pone a un ruteador tan sólo tiene ponderancia local, éste permite al usuario confirmar en qué ruteador está trabajando, en especial al tener varias sesiones remotas abiertas simultáneamente.

Para asignar un nombre a un ruteador se utiliza el comando **hostname**.

```
Router(config)#
Router(config)#hostname cancun
```

```
cancun(config)#
```

Al asignar nombre a un ruteador, el indicador cambia de inmediato, y también al conectarse vía Telnet a ese ruteador, el indicador muestra el nombre del mismo.

En la figura 4.5 se muestra la conexión Telnet al ruteador al que se le configuró con el nombre Cancún. (de hecho, cancun por razones obvias)

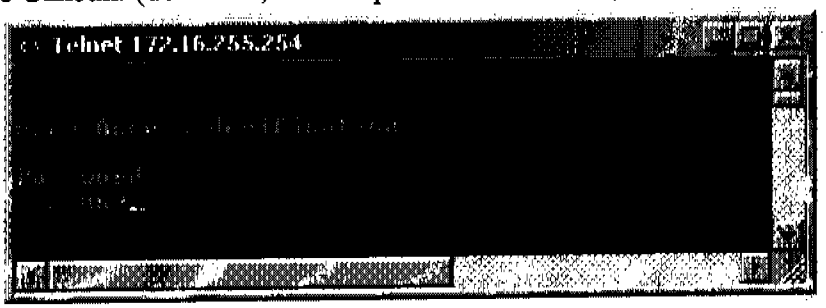


Figura 4.5 conexión por Telnet al ruteador Cancún

Nótese que el nombre del ruteador sigue teniendo alcance local. La sesión de Telnet se estableció por el IP de una interfase del ruteador (172.16.255.254.)

4.3.4 Claves de acceso

Uno de los puntos más importantes, y de los primeros que se deben atender, es la seguridad en el acceso al ruteador que se está configurando. Existen tres líneas de acceso al ruteador: Consola, Auxiliar y Telnet.

Para accesar al ruteador por medio de la consola o auxiliar tan solo es necesario conectarse al puerto RJ-45 correspondiente como se especifica en la sección 4.1.2 "Conexión a un Ruteador".

4.3.5 Consola

La conexión por consola permite iniciar una sesión sin necesidad de establecer una palabra clave, lo que es un riesgo a la seguridad que se debe evitar cuanto antes.

```
Router con0 is now available

Press RETURN to get started.

Router>enable
Router#
```

Lo único que se requirió para entrar a modo usuario, fue encender el ruteador y pulsar **[Enter]**; y para entrar a modo privilegiado, teclear el comando **enable**. ¡Aquí urge algo de seguridad!

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password consola
Router(config-line)#exit
```

Desde modo de configuración global se puede accesar el modo de configuración para líneas de acceso, una de ellas, la que se muestra: **console 0**. (Cisco enumera comenzando con cero.) El comando **login** indica que el momento de pedir la clave es al autentificarse, si no se pone este comando, el ruteador no pedirá la clave en ningún momento.

```
Router(config)#exit
Router#
Router#exit
Press RETURN to get started.
```

El comando **exit** sirve para salir de un nivel al nivel anterior.

[Enter]

```
User Access Verification

Password:
```

¡Mucho mejor! Ahora el ruteador verifica el acceso al modo usuario. Como el acceso en este ejemplo se está realizando por medio de la consola, la clave que se pide es la introducida a esa línea de acceso: "consola". Un detalle que confunde a quien está acostumbrado al estilo de Microsoft es que al teclear la clave no hay respuesta (ni siquiera con "*") en pantalla.

```
Password:
Router>enable
Router#
```

El acceso a modo usuario ya está regulado, pero de allí al modo privilegiado se sigue necesitando tan sólo un comando. (En esta misma sección se resuelve ese problema.)

4.3.6 Auxiliar

El uso de la línea de acceso auxiliar es muy similar al de la consola.

```
Router tty17 is now available

Press RETURN to get started.

[ Enter ]

Router>enable
% No password set
Router>
```

Para llegar a modo usuario tan sólo se requiere teclear **[Enter]**, pero esta vez no es tan fácil pasar de modo usuario a modo privilegiado. La línea auxiliar puede ser configurada para recibir con la ayuda de un módem accesos por vía telefónica, de modo que, es indispensable regular el acceso al modo privilegiado. Aparentemente, si no se ha puesto una palabra clave al puerto auxiliar, el ruteador no permite el acceso a modo privilegiado... (Aparentemente.)

Para establecer la palabra clave en la línea auxiliar el procedimiento es muy parecido al que se siguió para hacerlo en la consola.

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line aux 0
Router(config-line)#login
Router(config-line)#password auxiliar
Router(config-line)#exit
Router(config)#exit
Router#exit
```

Ahora se debe de poder accesar el modo privilegiado. ¿O no?

```
Router tty17 is now available
Press RETURN to get started.
[ Enter ]
User Access Verification
Password:
Router>
```

Esta vez sí hubo verificación a la línea de acceso.

```
Router>enable
% No password set
Router>
```

¿Queeeeé? ¿De todos modos no se puede accesar a modo privilegiado? –No. Para accesar al modo privilegiado cuando la conexión al ruteador se hace por un medio remoto, es necesario que exista una palabra clave específicamente puesta para diferenciar entre usuarios normales y usuarios privilegiados. El establecimiento de dicha palabra clave se discute en esta misma sección.

Nota: Cuando no hay una palabra clave para el modo privilegiado pero la palabra clave para la consola ha sido establecida, el ruteador pide dicha palabra para accesar al modo privilegiado desde la línea auxiliar.

4.3.7 Telnet

La conexión por Telnet es sumamente útil ya que permite accesar a un dispositivo remotamente a través de la red. Para poder hacerlo, es necesario tener conectividad con el dispositivo.

Es posible hacer Telnet a un dispositivo remoto desde un *host* o desde otro dispositivo. La figura 4.6 muestra el proceso desde una computadora.

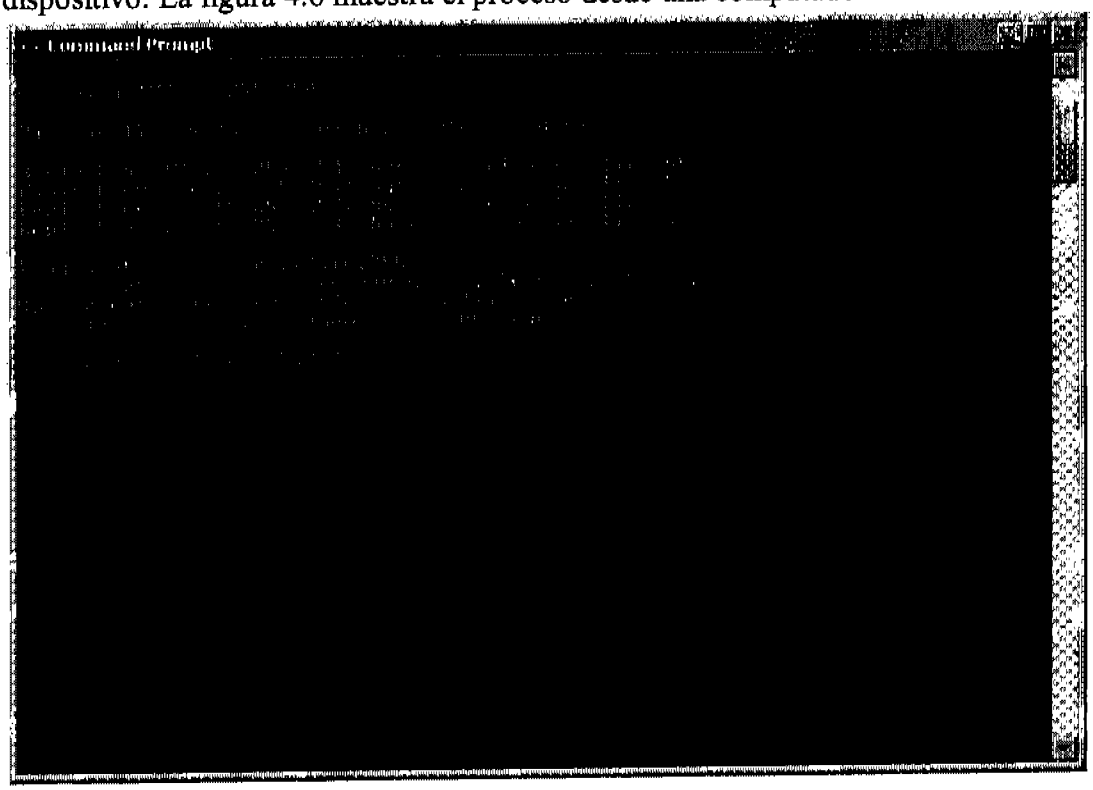


Figura 4.6 Telnet desde una computadora al ruteador 172.16.255.254

En la figura 4.6 se puede ver que al hacer ping al puerto 172.16.255.254 del ruteador sí se tiene conectividad. Hacer una prueba de conectividad antes de intentar establecer una sesión por Telnet es una buena práctica. De ese modo, es posible identificar fácilmente errores no relacionados específicamente con el protocolo Telnet. Para establecer la sesión Telnet se escribe el comando Telnet seguido del IP de una de las interfases del dispositivo al que se desea accesar. En la figura 4.7 se muestra la pantalla siguiente a la que se muestra en la figura 4.6.

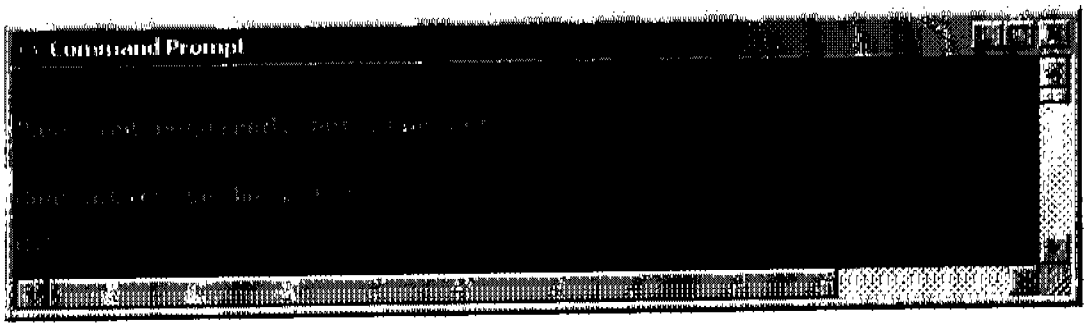


Figura 4.7 Intento de hacer Telnet a un ruteador que no tiene clave de acceso a Telnet.

Como se puede ver en la figura 4.7 no es posible establecer una sesión de Telnet en un ruteador que no tiene especificada una palabra clave para regular la conexión por la línea de acceso Telnet.
Hay que arreglar ese problema:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password remota
Router(config-line)#exit
Router(config)#exit
Router#
```

El comando **vty 0 4** hace referencia a la línea de acceso "*Virtual TeletYpe*" mejor conocida como Telnet y se utilizan los parámetros **0 4** para indicar que se accesa a todas las sesiones que se hagan por Telnet (5 de manera predeterminada.)

Ahora que se ha fijado una clave para el acceso por Telnet, se obtiene la respuesta que se puede ver en la figura 4.8. (Al escribir la clave, ésta no se muestra en pantalla)

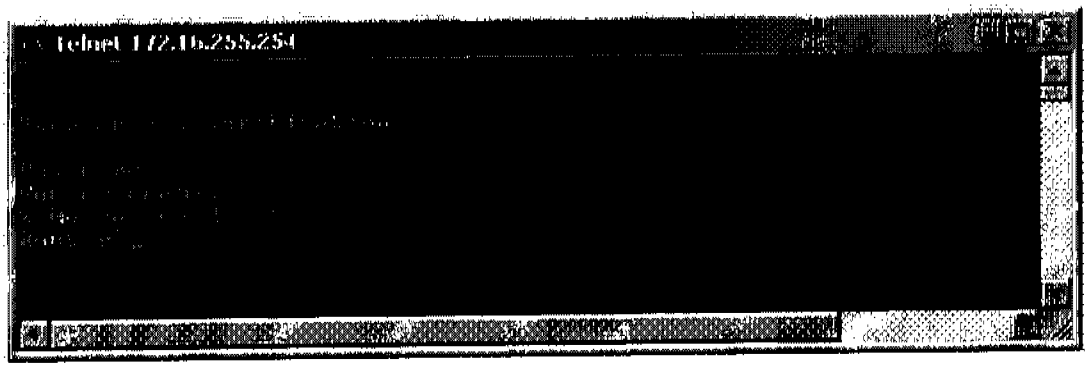


Figura 4.8 Sesión de Telnet.

Con la clave de Telnet configurada en el ruteador, es posible establecer la sesión. Sin embargo, una vez más se requiere que el ruteador tenga configurada una clave para el acceso a modo privilegiado para poder usarlo.

4.3.8 Modo de usuario privilegiado

¡Al fin! ¿Cómo se establece la clave de acceso al modo privilegiado? – para hacerlo se utilizan dos comandos: **enable password** y **enable secret**. De hecho, estos comandos no son indistintos y esto se ve en el siguiente ejemplo.

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable password privilegiado
Router(config)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#exit
```

¡Así de sencillo es poner la palabra clave de acceso al modo privilegiado! Ahora se comprobará su eficacia.

```
User Access Verification

Password:
```

Se introduce la clave de la línea de acceso, como la conexión se está haciendo por consola, la palabra clave es "consola", recuérdese que la pantalla no muestra como se teclea la palabra clave.

```
Router>
```

Acceso concedido. Ahora se intentará entrar al modo privilegiado.

```
Router>enable
Password:
```

El ruteador pide la palabra que se acaba de configurar, la palabra clave es "privilegiado".

```
Router#
```

Y... ¡listo! Se ha accesado al modo privilegiado. En la misma configuración del ruteador, ahora se establecerá la clave con el comando **enable secret**.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable secret privsecreta
Router(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
Router#exit
```

La clave "privsecreta" se ha establecido con el comando **enable secret**. El ruteador ahora tiene la palabra clave privilegiado, que se estableció utilizando **enable password** y la clave "privsecreta" que se estableció con **enable secret**. Al entrar de nuevo al ruteador se tiene:

```
Router con0 is now available

Press RETURN to get started.

User Access Verification

Password:
Router>
```

Al escribir la clave de línea de acceso "consola" se tuvo acceso al modo de usuario normal.

```
Router>enable
Password:
Password:
Password:
% Bad secrets
```

Al escribir la clave "privilegiado" (tres veces para descartar errores de tecleo), el mismo ruteador que la aceptó en el ejemplo anterior ahora no la acepta y, como es de esperarse al teclear la palabra "privsecreta":

```
Router>enable
Password:
Router#
```

Se cambia sin problemas al modo privilegiado.

Conclusión: si la palabra enable secret se ha especificado en el ruteador, ésta es la palabra que el ruteador pedirá para entrar a modo privilegiado. La palabra enable password solamente se pedirá si la palabra enable password se ha configurado y la enable secret no.

La palabra enable password se utiliza en ruteadores que no soportan la enable secret que son los que tienen IOS versión 10.3 y anteriores y los ruteadores que soportan la enable secret también soportan la enable password por compatibilidad con equipos viejos.

4.3.9 Encripción de claves

Uno de los comandos más útiles en la configuración y monitoreo de un ruteador es el comando **show** desde modo privilegiado y una de las opciones más populares es **show running-config** que muestra la configuración en RAM que el ruteador tiene.

```
Router#show running-config

Building configuration...

Current configuration:
!
version 11.0
service udp-small-servers
service tcp-small-servers
!
hostname Router
!
enable secret 5 $1$Jo/k$obZR9uKsVFC1W04JoFPu0/
enable password privileglado
!
!
interface Ethernet0
 no ip address
```

```
 shutdown
!
interface Serial0
 no ip address
 shutdown
 no fair-queue
!
interface Serial1
no ip address
 shutdown
!
!
line con 0
 password consola
 login
line 1 16
 transport input all
line aux 0
 password auxiliar
 login
 transport input all
line vty 0 4
 password remota
 login
!
end
```

Al pedirle al ruteador que muestre su RAM, éste lo hace sin recato alguno, o casi sin recato; si se busca en el desplegado anterior, se encontrarán todas las palabras claves que se pusieron en esta sección. Y todas están en texto claro, todas excepto una: La enable secret, la cual esta encriptada. La encripción de la palabra secreta está habilitada por *default* en los ruteadores Cisco pero es posible encriptar otras palabras claves utilizando el servicio de encripción

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#service password-encryption
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password merida
Router(config-line)#exit
Router(config)#line console 0
Router(config-line)#login
```

```
Router(config-line)#password yucatan
Router(config-line)#exit
Router(config)#exit
Router#
```

Ahora al pedir un despliegue de RAM:

```
Router#show run
Current configuration:
!
version 11.0
service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname Router
!
!
!
interface Ethernet0
 no ip address
 shutdown
!
interface Serial0
 no ip address
 shutdown
 no fair-queue
!
interface Serial1
 no ip address
shutdown
!
!
line con 0
 password 7 13081200020805
 login
line 1 16
 transport input all
line aux 0
 transport input all
line vty 0
 password 7 151F0E1E0D2E2A
 login
```

```
line vty 1
 password 7 13081200020805
 login
line vty 2
 password 7 141A171905002B
 login
line vty 3
 password 7 121400051B0F0D
 login
line vty 4
 password 7 151F0E1E0D2E2A
 login
!
end

Router#
```

Mucho más seguro en definitiva.

4.4 Mensajes de Acceso

Como complemento a la seguridad que las palabras claves dan, los ruteadores Cisco pueden ser configurados para desplegar un mensaje en determinados puntos de acceso.

El comando a usar es **banner** desde modo de configuración global.

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#banner ?
  LINE     c banner-text c, where 'c' is a delimiting character
  exec     Set EXEC process creation banner
  incoming  Set incoming terminal line banner
  login    Set login banner
  motd     Set Message of the Day banner

Router(config)#banner
```

Al pedir ayuda sobre el comando **banner**, el ruteador muestra la sintaxis que se debe seguir para establecerlo "c banner-text c" en donde la "c" es un caracter delimitante. En otras palabras, se pone un caracter para indicar que el mensaje inicia y el mismo

caracter para indicar que el mensaje termina. Dicho caracter se especifica en el comando.

La ayuda también muestra los cuatro puntos de acceso en los que se puede desplegar un mensaje.

Exec.- Despliega un mensaje cuando el usuario accesa al modo de ejecución (usuario normal) desde alguna línea de acceso (Telnet, consola o auxiliar.)

Incoming.- Despliega un mensaje en las terminales que se conectan por reverse Telnet al ruteador. Este mensaje normalmente provee instrucciones a los usuarios acerca de la conexión por reverse Telnet.

Login.- Despliega un mensaje inmediatamente antes de solicitar la autentificación.

Motd.- Message of the Day. Este es el tipo de mensaje mayormente utilizado ya que se despliega al conectarse por cualquier medio al ruteador.

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#banner motd #
Enter TEXT message.  End with the character '#'.
[ Enter ]
Este es el mensaje del dia
Bienvenido a trabajar administrador de la red
[ Enter ]
#
Router(config)#
```

Cuando se introdujo el comando **banner motd** #, además de especificar el momento en que se debe desplegar el mensaje, también se definió el caracter "#" como marcador de inicio y de término del mensaje. Gracias a que existe un caracter que delimita el mensaje, el mensaje puede incluir espacios y aún líneas en blanco.

```
Router con0 is now available
Press RETURN to get started.

Este es el mensaje del dia
Bienvenido a trabajar administrador de la red

Router>
```

Al hacer la conexión al ruteador configurado con el banner motd, éste se despliega al iniciar la sesión. Nótese que el mensaje incluye las líneas en blanco que se configuraron.

4.5 Interfases del Ruteador

La tabla 4.1 en la sección "Estructura de los Ruteadores Cisco" muestra algunos modelos de ruteadores y las diferentes interfases que cada uno de ellos tiene. La configuración de interfases es, sin duda, uno de los aspectos más importantes en el manejo de ruteadores ya que la función de un ruteador es dividir dominios de *broadcast* y proveer los medios para la interacción de redes, y estas funciones simplemente no serían posibles sin interfases a las cuales las redes se pudieran conectar.

Son pocos los parámetros que se deben configurar para proveer conectividad a una interfase y estos incluyen:

- Dirección lógica de la interfase.- En el caso de TCP/IP, esta dirección es el IP. Es importante recordar que cada interfase en uso debe tener su propia dirección lógica y que dichas direcciones deben pertenecer a distintas sub-redes.

- Ancho de banda.- El ancho de banda es la capacidad del medio para transmitir cierta cantidad de datos en cierta cantidad de tiempo.

- Tipo de medio de transmisión.- Este puede ser par trenzado, fibra óptica, etc. Normalmente el tipo de medio se auto-detecta pero es posible configurarlo de manera manual.

Para entrar a configurar una interfase, solamente se necesita introducir el nombre de la interfase desde modo de configuración global. Esto pudiera entrañar un pequeño detalle de confusión: las interfases varían de nombre según la serie del ruteador en el que se encuentren, así, las interfases en un ruteador 2500 se llaman *Ethernet* 0, Serial 0 y Serial 1, mientras que en un ruteador 2600 se llaman *Fast Ethernet* 0/0, *Fast Ethernet* 0/1, Serial 0/0 y Serial 0/1. ¿Cómo saber la diferencia? Una manera infalible de conocer el nombre de una interfase, es ver físicamente el rótulo correspondiente en el ruteador. sin embargo, una manera más general (y más técnica) de hacerlo es siguiendo el formato:

interface [tipo de interfase] [número de la interfase]

En dónde el número para las interfases fijas en un ruteador simplemente se obtiene de una enumeración de los puertos comenzando con 0 y el número para las interfases modulares (en ruteadores de las series 2600, 3600, 4000 y 7000) se numeran utilizando el formato:

[ranura] / [puerto]

Por lo que el nombre en estos ruteadores es: **interface [tipo] [ranura]/[puerto]**

Todas las interfases en los ruteadores vienen apagadas de fábrica y hay que prenderlas cuando se quieran utilizar. Recuérdese que para hacer lo contrario a la gran mayoría de los comandos en el IOS, se utiliza el mismo comando pero precedido de la palabra **no**. El comando para apagar una interfase es **shutdown**, por lo tanto el comando para encenderla es ... ¡correcto! **no shutdown**.

Una consideración importante al configurar las interfases seriales es que este tipo de conexiones siempre tienen un extremo llamado DTE (*Data Terminal Equipment*) y un extremo llamado DCE (*Data Communications Equipment.*) El extremo DCE debe de proveer el ritmo de la comunicación a través de un reloj que tan sólo afecta a esta conexión. Normalmente el proveedor del servicio de comunicación maneja el DCE. Pero, cuando se conectan dos interfases seriales, una de ellas debe funcionar como DCE y proveer dicho reloj.

No se olvide que la ayuda interconstruida puede ser, precisamente, de mucha ayuda.

```
Router(config)#interface ?
  Async            Async interface
  BVI              Bridge-Group Virtual Interface
  Dialer           Dialer interface
  Ethernet         IEEE 802.3
  Group-Async      Async Group Interface
  Lex              Lex interface
  Loopback         Loopback Interface
  Null             Null interface
  Port-channel     Ethernet Channel of Interfaces
  Serial           Serial
  Tunnel           Tunnel interface
  Virtual-Template  Virtual Template interface
  Virtual-TokenRing  Virtual TokenRing

Router(config)#interface ethernet ?
<0-0>  Ethernet interface number

Router(config)#interface ethernet 0 ?
  <cr>

Router(config)#interface ethernet 0 [ Enter ]
Router(config-if)#
```

Tal como se esperaba, el comando para entrar a configurar la interfase tiene el formato: **interface [tipo de interfase] [número de la interfase]**. Además, por la ayuda ofrecida por el ruteador se puede ver que este ruteador en particular tan sólo tiene una interfase *Ethernet* ya que las opciones para escoger número de interfase fueron cero o cero.

```
Router(config-if)#band?
bandwidth

Router(config-if)#bandwidth ?
  <1-10000000>  Bandwidth in kilobits

Router(config-if)#bandwidth 64
```

Es importante que se note que el ancho de banda se configura en Kilo*bit*s.
Al pedir un listado de todos los comandos disponibles dentro del modo de configuración de la interfase *Ethernet* 0 se obtiene:

```
Router(config-if)#?
  Interface configuration commands:
  access-expression        Build a bridge boolean access expression
  appletalk                Appletalk interface subcommands
  arp                      Set arp type (arpa, probe, snap) or timeout
  autodetect               Autodetect Encapsulations on Serial Interface
  backup                   Modify dial-backup parameters
  bandwidth                Set bandwidth informational parameter
  bridge-group             Transparent bridging interface parameters
  carrier-delay            Specify delay for interface transitions
  cdp                      CDP interface subcommands
  clock                    Configure serial interface clock
  compress                 Set serial interface for compression
  custom-queue-list        Assign a custom queue list to an interface
  dce-terminal-timing-enable  Enable DCE terminal timing
  decnet                   Interface DECnet config commands
  default                  Set a command to its defaults
  delay                    Specify interface throughput delay
  description              Interface specific description
  dialer                   Dial-on-demand routing (DDR) commands
  dialer-group             Assign interface to dialer-list
  down-when-looped         Force looped serial interface down
  dxi                      ATM-DXI configuration commands
  encapsulation            Set encapsulation type for an interface
```

```
exit                Exit from interface configuration mode
fair-queue          Enable Fair Queuing on an Interface
full-duplex         Configure full-duplex operational mode
half-duplex         Configure half-duplex and related commands
help                Description of the interactive help system
hold-queue          Set hold queue depth
idle-character      Set idle character type
ignore-dcd          Ignore dcd
invert              Serial invert modes
ip                  Interface Internet Protocol config commands
ipx                 Novell/IPX interface subcommands
keepalive           Enable keepalive
llc2                LLC2 Interface Subcommands
load-interval       Specify interval for load calculation for an
                    Interface
logging             Configure logging for interface
loopback            Configure internal loopback on an interface
mac-address         Manually set interface MAC address
mop                 DEC MOP server commands
mtu                 Set the Interface Maximum Transmission Unit (MTU)
netbios             Use a defined NETBIOS access list or enable
                    name-caching
no                  Negate a command or set its defaults
nrzi-encoding       Enable use of NRZI encoding
ntp                 Configure NTP
ppp                 Point-to-Point Protocol
priority-group      Assign a priority group to an interface
pulse-time          Enables pulsing of DTR during resets
random-detect       Enable Random Early Detection (RED) on an
                    Interface
shutdown            Shutdown the selected interface
smds                Modify SMDS parameters
smrp                Simple Multicast Routing Protocol interface
                    subcommands
snapshot            Configure snapshot support on the interface
snmp                Modify SNMP interface parameters
timeout             Define timeout values for this interface
traffic-shape       Enable Traffic Shaping on an Interface or
                    Sub-Interface
transmit-interface  Assign a transmit interface to a receive-only
                    Interface
tx-queue-limit      Configure card level transmit queue limit
```

Por supuesto que estas opciones cambian de modelo a modelo y según la interfase de que se trate, pero los mostrados dan una idea de lo versátil que puede ser una interfase.

```
Router(config-if)#
Router(config-If)#ip address 172.16.0.1 255.255.0.0
Router(config-if)#no shutdown
00:32:32 %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, changed state to up
00:32:32 %LINK-3-UPDOWN:  Interface Ethernet0, changed state to up
Router(config-if)#exit
```

Para configurar la dirección lógica de la interfase se utilizó el comando **ip address [ip] [máscara de sub-red]**. El comando **no shutdown** encendió la interfase.

Ahora se configura una interfase serial.

```
Router(config)#int s 0
```

El único comando desde modo de configuración global en que cada palabra comienza con las letras mostradas es **interface serial 0** por lo que al dar **[Enter]** no hay ambigüedad así que el ruteador reconoce y ejecuta el comando.

```
Router(config-if)#ip address 172.17.0.1 255.255.0.0
Router(config-If)#clock rate ?
  Speed (bits per second)
  1200
  2400
  4800
  9600
  19200
  38400
  56000
  64000
  72000
  125000
  148000
  250000
  500000
  800000
  1000000
  1300000
  2000000
  4000000
```

```
<300-8000000>  Choose clockrate from list above

Router(config-if)#clock rate 64000
Router(config-if)#
```

En la configuración que se muestra, al momento de conectar el ruteador se puso el extremo DCE en esta interfase y por eso se requiere configurar el reloj. Si se hubiera puesto el extremo DTE en esta interfase, el ruteador indicaría un error como el siguiente:

```
%Error: This command applies only to DCE interfaces
```

Muchos administradores simplemente tratan de configurar el reloj a todas las interfases seriales ya que si no obtienen un error es por que se necesitaba un reloj, y si se obtiene el error, simplemente no se necesitaba y no se configura. Personalmente, prefiero saber qué interfases son DCE.

```
Router(config-if)#bandwidth 64
Router(config-if)#no shutdown
00:41:23 %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to up
00:41:23 %LINK-3-UPDOWN:  Interface Serial0, changed state to up

Router(config-if)#exit
Router(config)#exit
```

Se han configurado la interfase serial 0 y la interfase *Ethernet* 0. **show run** muestra la configuración:

```
Router#show run
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
!
!
ip subnet-zero
!
interface Ethernet0
 ip address 172.16.0.1 255.255.0.0
```

```
 no ip directed-broadcast
!
interface Serial0
 bandwidth 64
 ip address 172.17.0.1 255.255.0.0
 no ip directed-broadcast
 no ip mroute-cache
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
!
no ip classless
!
!
!
line con 0
line aux 0
line vty 0 4
!
end
Router#
```

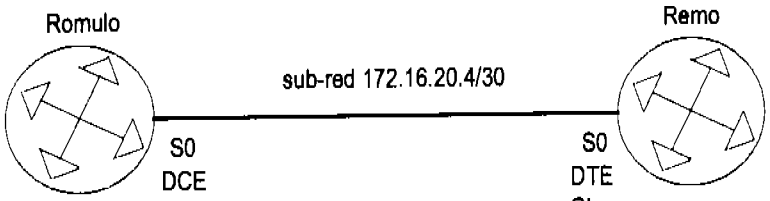
Nótese el estado y la configuración de cada interfase, inclusive de la serial 1 que no se configuró.

Causas muy comunes de errores en los exámenes de certificación son la omisión de los comandos **no shutdown** y **clock rate**, de modo que hay que ser muy cuidadoso en ese aspecto.

En el escenario 4.1 se ve la configuración de un par de ruteadores con los comandos vistos hasta el momento y algunos nuevos.

Escenario 4.1

Configurar los ruteadores Rómulo y Remo con los datos que se muestran en la figura 4.9



Claves:
enable: rey
secret: Roma
consola: imperio
aux: Quirino
telnet: Marte
banner motd: El rutedor Romulo es de acceso restringido

Claves:
enable: Tiber
secret: mitología
consola: loba
aux: poder
telnet: gemelo
banner motd: Bienvenido al ruteador Remo

Figura 4.9 Escenario 4.1 a ser configurado

La configuración de Rómulo es:

Router Con0 is now available

Press RETURN to get started!

Router>**enable**
Router#**config t**
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#**hostname Romulo**
Romulo(config)#**banner motd # El ruteador Romulo es de acceso restringido #**
Romulo(config)#**line console 0**
Romulo(config-line)#**login**
Romulo(config-line)#**pass imperio**
Romulo(config-line)#**line aux 0**
Romulo(config-line)#**login**
Romulo(config-line)#**pass Quirino**
Romulo(config-line)#**line vty 0 4**
Romulo(config-line)#**login**
Romulo(config-line)#**pass Marte**
Romulo(config-line)#**exit**
Romulo(config)#**enable pass rey**
Romulo(config)#**enable secret Roma**
Romulo(config)#**int s0**
Romulo(config-if)#**ip address 172.16.20.5 255.255.255.252**
Romulo(config-if)#**clock rate 64000**
Romulo(config-if)#**description conexion a rutedor Remo**

```
Romulo(config-lf)#no shut
04:40:22 %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to up
04:40:22 %LINK-3-UPDOWN:  Interface Serial0, changed state to up

Romulo(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

Romulo#copy running-config startup-config
Destination filename [startup-config]?[ Enter ]
Warning: Attempting to overwrite an NVRAM configuration
previously written by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...

[OK]

Romulo#
```

Hay tres detalles nuevos en la configuración de Rómulo.

El primero es que al terminar de configurar cada una de las líneas de acceso, no se hizo un **exit** para volver al nivel anterior y después un acceso a la siguiente línea de acceso. En realidad si se hizo, sólo que de manera implícita. Cuando el indicador al que se va es el mismo que donde se está, es posible tan sólo indicar a donde se va y el ruteador lo acepta.

El segundo es el comando **description** que no tiene relevancia alguna a nivel código pero es útil para que el administrador haga comentarios acerca de una interfase. Estos comentarios se ven al pedir un desplegado de la configuración utilizando el comando **show running-config** desde el modo de usuario privilegiado.

El tercero y último detalle nuevo es el comando **copy running-config startup-config**; se recordará que al trabajar en un ruteador se trabaja en RAM, en la configuración running-config. De modo que al apagar el ruteador, la configuración se perderá, a menos que esta configuración se copie a la NVRAM (startup-config.) Al hacerlo, la próxima vez que se arranque ese ruteador se cargará la configuración recientemente modificada.

Un detalle que no es nuevo, pero vale la pena mencionar es que las claves de acceso son sensibles a las mayúsculas por lo que "roma" no es lo mismo que "Roma" cuando se trata de una clave, sin embargo "configure terminal" es lo mismo que "CoNfIGUre terMINal".

La configuración de Remo se ve a continuación:

```
Router Con0 is now available
```

```
Press RETURN to get started!

Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Remo
Remo(config)#banner motd # Bienvenido al ruteador Remo #
Remo(config)#line console 0
Remo(config-line)#login
Remo(config-line)#pass loba
Remo(config-line)#line aux 0
Remo(config-line)#login
Remo(config-line)#pass poder
Remo(config-line)#line vty 0 4
Remo(config-line)#login
Remo(config-line)#pass gemelo
Remo(config-line)#exit
Remo(config)#enable pass Tiber
Remo(config)#enable secret mitologia
Remo(config)#int s0
Remo(config-if)#ip address 172.16.20.6 255.255.255.252
Remo(config-if)#description conexion a rutedor Romulo
Remo(config-if)#no shut
04:40:25 %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to up
04:40:25 %LINK-3-UPDOWN:  Interface Serial0, changed state to up

Remo(config-if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

Remo#copy running-config startup-config
Destination filename [startup-config]?[ Enter ]
Warning: Attempting to overwrite an NVRAM configuration
previously written by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...

[OK]
Remo#
```

En Remo no fue necesario configurar el reloj para la conexión por S0 (¡Claro! Ésta es una interfase DTE.)

Las direcciones fueron calculadas para satisfacer el número requerido en el segmento. A modo de ejercicio se pueden comprobar dichas direcciones y que pertenezcan a la sub-red que se pide.

El éxito del escenario prácticamente se reduce a comprobar que hay conectividad entre ruteadores.

```
Remo#ping 172.16.20.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.20.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent(5/5),round-trip min/avg/max = 9/9/10 ms
Remo#
```

De Remo a Rómulo sí hay conectividad.

```
Romulo#ping 172.16.20.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.20.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/9/9 ms
Romulo#
```

Y de Rómulo a Remo también hay conectividad.

Al pedir el desplegado de RAM de Rómulo se observa:

```
Romulo#sh run
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Romulo
!
enable secret 7 13081200020805
enable password rey
!
ip subnet-zero
```

```
!
interface Ethernet0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Serial0
 description conexion a rutedor remo
 ip address 172.16.20.5 255.255.255.252
 no ip directed-broadcast
 clock rate 64000
 no ip mroute-cache
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
!
no ip classless
!
banner motd #
 El ruteador Romulo es de acceso restringido
#
!
!
!
line con 0
  password imperio
  login
line aux 0
  password Quirino
  login
line vty 0 4
  password Marte
  login
!
end
Romulo#
```

En este desplegado no hay forma de saber si S0 es DCE o DTE. Ese parámetro se determina al hacer la conexión en los ruteadores, pero hay una forma de averiguarlo

desde el ruteador, y es a través del comando **show controllers** desde modo privilegiado.

```
Romulo#show controllers serial 0
HD unit 0, idb = 0x1076CC, driver structure at 0x10CB58
buffer size 1524  HD unit 0, V.35 DCE cable
cpb = 0x41, eda = 0x4e4a, cda = 0x49be
RX ring with 16 entries at 0x614800
```

Este comando da muchísima información además de la que se muestra, pero el desplegado se corta por motivos de espacio.

Un comando que conviene explorar antes de presentar el examen es el comando **show** desde el modo privilegiado, y sus variantes: **show interface, show controllers, show ip interface, show versión, show history, show proceses, show ip, show terminal, show protocols, show IP protocols** etc. La mayoría de los simuladores soportan por lo menos los comandos explícitamente listados.

Capítulo 5

Métodos y Protocolos de Ruteo

5.1 Introducción

En este capítulo se discute brevemente el funcionamiento y la configuración de los métodos y algunos de los protocolos más importantes de ruteo. Si bien existen otros protocolos ruteables, el objetivo de este manual es explorar TCP/IP, de modo que, al hablar de ruteo, se está hablando de ruteo IP.

Para hablar de ruteo es necesario comprender la función de los ruteadores. Recuérdese que los ruteadores son dispositivos diseñados tanto para dividir dominios de *broadcast*, como proveer intercomunicación entre distintos dominios de *broadcast*. Mientras que los *switches*, que son dispositivos de capa 2 se basan en el MAC de un dispositivo para tomar sus decisiones de envío; los ruteadores, que son dispositivos de capa 3, se basan en direcciones lógicas para hacerlo. Los *switches* ven dispositivos mientras que los ruteadores ven redes.

Un ruteador ve por *default* las redes que tiene directamente conectadas a sus puertos pero para ver el resto de las redes o subredes en determinado escenario, depende de los protocolos de ruteo.

Es importante diferenciar entre protocolos ruteables y protocolos de ruteo;

Los protocolos ruteables son simplemente protocolos de comunicación capaces de transitar por un ruteador. No todos los protocolos tienen esa capacidad, más bien son pocos los protocolos ruteables, los protocolos ruteables más importantes son TCP/IP, IPX/SPX y Appletalk (en el sentido estricto, éstos no son protocolos sino conjuntos de protocolos o *protocol stacks*.) Cabe mencionar al más famoso de los protocolos no ruteables: NetBEUI de Microsoft. A pesar de que NetBEUI es un protocolo ligero y eficiente que no causa sobrecarga al procesador de los dispositivos, fácil de utilizar y con un sistema de direccionamiento basado en nombres, no es un protocolo que entiendan los ruteadores y por lo tanto es imposible comunicarse utilizando NetBEUI entre distintas redes, lo que confina a un protocolo tan versátil y eficiente a un ambiente LAN y plataformas Microsoft exclusivamente.

Los protocolos de ruteo son aquellos diseñados para permitir que un ruteador descubra la mejor ruta que un paquete debe seguir para arribar a su destino. Normalmente estos protocolos no llegan a salir del ambiente WAN hacia las LANs y los usuarios no se percatan de su existencia más que por sus beneficios indirectos. La mejor ruta para que un paquete llegue a su destino no siempre es la "mejor ruta"; diferentes protocolos de ruteo consideran diferentes parámetros para determinar la mejor ruta. Por ejemplo, uno de los protocolos más utilizados es RIP (*Routing Information Protocol*), y RIP se basa tan sólo en la cuenta de saltos o hops para determinar la mejor ruta. Un salto o hop es cuando el paquete pasa por un ruteador, entonces RIP se basa en el número de ruteadores que un paquete debe cruzar para llegar a su destino.

Véase la figura 5.1. En ella se muestran dos caminos posibles para que un paquete vaya de "A" a "B" uno por la línea sólida y otro por la línea punteada. Si se toma la cuenta de hops como único parámetro de decisión para determinar la mejor ruta. Es fácil ver que la mejor ruta a seguir es por el camino de la línea sólida. Pero... ¿Cuál sería el mejor camino si la línea puntada representara una conexión sobre fibra óptica y la línea sólida representara la misma distancia sobre línea telefónica categoría 3?

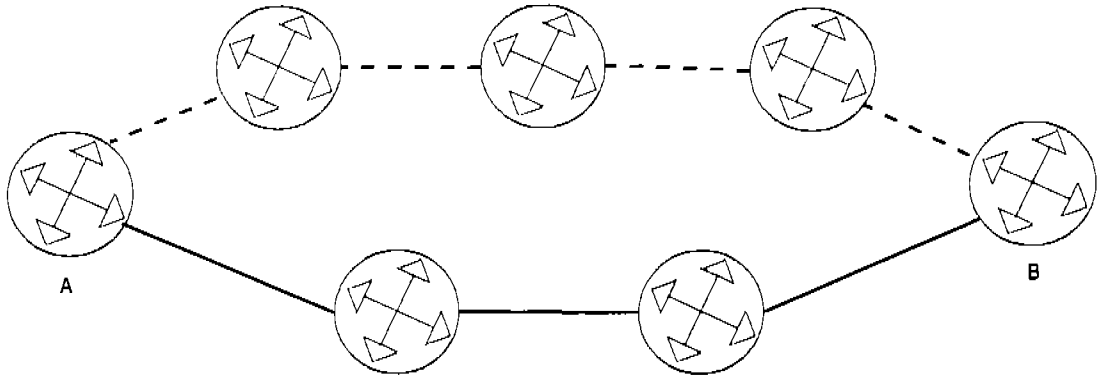


Figura 5.1 ¿Cuál es la mejor ruta?

Bueno, ya se dijo antes, la mejor ruta es por la línea sólida ya que el parámetro a considerar es únicamente la cuenta de hops. Este ejemplo muestra cuán importante es el papel del diseñador de redes para determinar el protocolo de ruteo a utilizar y los parámetros a considerar en distintos escenarios.

5.2 Métodos de Ruteo

Para determinar las rutas a seguir cuando un paquete llega a un ruteador, éste se basa en sus tablas de ruteo, que simplemente son listados de los identificadores de red (*Net ID*) de las redes o sub-redes con las cuales se busca tener conectividad y la dirección que se debe seguir para llegar a ellas. Las tablas de ruteo pueden ser configuradas de tres formas: a través del ruteo estático, a través del ruteo por *default* o a través del ruteo dinámico.

5.3 Ruteo Estático

La manera más directa en la que se le puede indicar a un ruteador la ruta que los paquetes con distintos destinos deben seguir es la configuración manual o estática.

En la configuración manual los parámetros a considerar para la elección de la mejor ruta (que muchas veces es también la única ruta) son absolutamente a criterio del administrador de la red.

Como es de esperarse, el ruteo estático no consume tiempo de procesador y por lo mismo no provoca carga alguna al mismo. Además, si se le utiliza correctamente, puede ser el más adecuado en cualquier escenario ya que ningún protocolo de ruteo, por complejo que éste sea, puede tomar en cuenta tantos factores y parámetros para la determinación de la mejor ruta como una persona. El ruteo estático no utiliza ningún tipo de paquete para sincronizar las tablas de ruteo de los ruteadores, ya que se configuran manualmente uno por uno y no requieren compartir o que se les comparta información de ruteo. El administrador de la red puede decidir qué ruteadores pueden tener acceso a ciertas redes e implementarlo directamente en las tablas de ruteo. Todo esto, hace del método estático uno seguro, versátil y... ¡Agobiante!

Es claro que al utilizar el ruteo estático, cada ruteador debe ser configurado manualmente y si la red tiene decenas, cientos o hasta miles de sub-redes, esta tarea se vuelve pesada o hasta imposible ya que habrá decenas, cientos o hasta miles de ruteadores con decenas, cientos o hasta miles de entradas en cada una de sus tablas de ruteo. Después de configurar las tablas de ruteo en muchos ruteadores, la adición de un ruteador o de una red y la consecuente actualización de las tablas ha de ser una pesadilla.

El ruteo estático es, sin embargo, la mejor manera de configurar una red pequeña de hasta 5 ó 6 ruteadores con pocas redes.

Para introducir una ruta en la tabla de ruteo utilizando el método estático, se utiliza, desde modo de configuración global, el comando:

ip route [red de destino] [máscara de la red de destino] [ip del siguiente ruteador en la ruta hacia la red de destino o interfase local por la que se debe enviar el paquete para que éste llegue a la red de destino] [distancia administrativa] [bandera de permanencia en la tabla de ruteo]

Este comando luce intimidante a primera vista, pero al aplicarlo puede verse tan sencillo como:

ip route 172.16.30.0 255.255.255.0 172.16.10.1

En este comando, la red a la que se pretende llegar es la 172.16.30.0 con una máscara de 24 *bits*. Es importante que se note que en este parámetro se utiliza un identificador de red de acuerdo a la máscara y no un IP asignable a un *host*. Para llegar a dicha red, el paquete se debe enviar por medio de la interfase que tenga el IP 172.16.10.1. Esta interfase tiene que ser visible al ruteador, es decir tiene que estar directamente conectada a él y en el mismo segmento que alguna de sus interfases. La distancia administrativa y la bandera de permanencia son opcionales.

La distancia administrativa es un valor numérico que cada protocolo de ruteo tiene y que el ruteador utiliza para determinar la prioridad en que los utilizará en caso de

existir más de una ruta para el mismo destino por diferentes métodos de ruteo. La distancia administrativa de las entradas hechas por ruteo estático es, por *default*, 1 para las rutas que especifiquen el siguiente hop (como en el comando anterior) y cero para las rutas que especifiquen la interfase local por la que se debe enviar el paquete, como en el comando:

ip route 172.16.30.0 255.255.255.0 Ethernet 0

La bandera de permanencia simplemente dice que esta entrada debe permanecer en la tabla de ruteo aún si la ruta resulta inaccesible por cualquier motivo. En caso de estar apagada, la ruta desaparecerá de la tabla de ruteo cuando la ruta se vuelva inaccesible.

Considérese el mapa de la figura 5.2 para el siguiente ejemplo de ruteo.

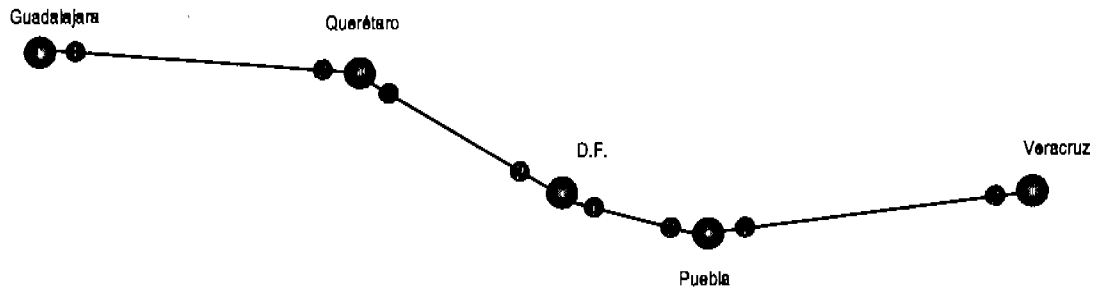


Figura 5.2 Un ruteo por México

Supóngase que con base en Puebla se desea ir al D.F. la tabla de ruteo estático diría algo como: "Para ir al D.F. se debe salir por el punto 2 de Puebla" o "Para ir al D.F. se debe ir por el punto 1 del D.F." (Éste último enunciado no es muy lógico al rutear por carreteras pero es el más utilizado al hacerlo en la red.)

Si desde Puebla se desea ir a Querétaro, la tabla de ruteo diría algo así: "Para llegar a Querétaro se debe ir por el punto 1 del D.F." y para ir a Guadalajara: "Para llegar a Guadalajara se debe ir por el punto 1 del D.F.".

La tabla completa para Puebla sería así:

D.F.	vía	1 D.F.
Querétaro	vía	1 D.F.
Guadalajara	vía	1 D.F.
Veracruz	vía	2 Veracruz

Como se puede apreciar en el ejemplo, el ruteo estático tan solo dice por donde se debe ir, considerando las direcciones directamente visibles. Como diciendo: "Llegando a ese punto. Pregunte por más indicaciones"

Escenario 5.2

Configurar los dispositivos de la figura para proveer conectividad entre todos los *hosts*.

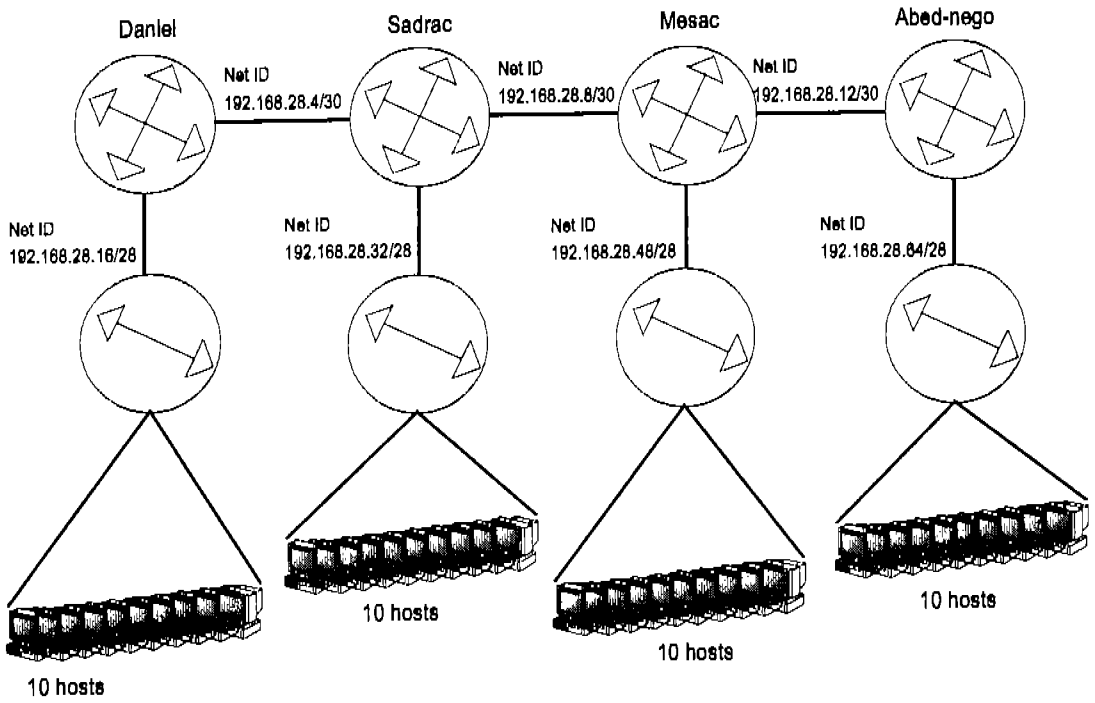


Figura 5.3 Escenario 5.2 Considérese que los ruteadores son 2501

A manera de práctica se pueden recalcular los IP's que se asignaron en el escenario 5.2 por medio de VLSM. En este escenario se tomará la configuración de fábrica de los *switches*. La elección de la red a subdividir es arbitraria, así como lo es la elección de las interfases a utilizar en cada ruteador. Personalmente, prefiero conectar un puerto serial 0 con un serial 1 cuando conecto ruteadores entre sí y así, siempre asigno el DCE al serial 0.

La configuración de Daniel es:

```
Router Con0 is now available

Press RETURN to get started!

Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname danniel
```

Hay algunos detalles que sólo la práctica (incluso en un simulador) puede aclarar. Uno de ellos es qué hacer al cometer un error al asignarle el nombre al ruteador. En el caso específico del nombre, tan sólo se le sobrepone el nombre correcto.

```
danniel(config)#hostname Daniel
Daniel(config)#banner motd # Ruteador Daniel #
Daniel(config)#enable password beltsasar
Daniel(config)#enable secret babilonia
Daniel(config)#line console 0
Daniel(config-line)#login
Daniel(config-line)#password leones
Daniel(config-line)#line aux 0
Daniel(config-line)#login
Daniel(config-line)#password fosa
Daniel(config-line)#line vty 0 4
Daniel(config-line)#login
Daniel(config-line)#password principe
Daniel(config-line)#exit
Daniel(config)#interface e0
Daniel(config-if)#ip address 192.168.28.17 255.255.255.240
Daniel(config-if)#description conexion a la lan 192.168.28.16
Daniel(config-if)#no shutdown
00:32:23 %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, changed state to up
00:32:23 %LINK-3-UPDOWN: Interface Ethernet0, changed state to up
```

Una buena práctica es asignarle a la interfase del ruteador la primera IP disponible en su segmento. De hecho, es bueno asignar IP´s comenzando con los dispositivos más cercanos a la capa de *core* en el modelo jerárquico de Cisco.

```
Daniel(config-if)#interface s0
Daniel(config-if)#ip address 192.168.28.5 255.255.255.252
Daniel(config-if)#clock rate 64000
Daniel(config-if)#description conexion a Sadrac
Daniel(config-if)#no shutdown
00:35:21 %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to up
00:35:21 %LINK-3-UPDOWN: Interface Serial0, changed state to up

Daniel(config-if)#exit
```

El ruteador Daniel, no necesita que se le configuren las redes 192.168.28.4 ó 192.168.28.16 ya que las ve directamente. Por lo tanto hay que dar de alta las redes 192.168.28.8, 12, 32, 48 y 64 con sus respectivas máscaras.

```
Daniel(config)#ip route 192.168.28.8 255.255.255.252 192.168.28.6
Daniel(config)#ip route 192.168.28.12 255.255.255.252 192.168.28.6
```

```
Daniel(config)#ip route 192.168.28.33 255.255.255.240 192.168.28.6
```

¡Un momento! No se debe de poner un IP asignable a un *host* sino el identificador de una red. No es .33 sino .32. Para corregir el error, en el caso de las tablas de ruteo es indispensable borrar la entrada errónea antes de introducir la correcta y para hacerlo se utiliza exactamente el mismo comando con el error pero precedido de la palabra "no".

```
Daniel(config)#no ip route 192.168.28.33 255.255.255.240 192.168.28.6
Daniel(config)#ip route 192.168.28.32 255.255.255.240 192.168.28.6
Daniel(config)#ip route 192.168.28.48 255.255.255.240 192.168.28.6
Daniel(config)#ip route 192.168.28.64 255.255.255.240 192.168.28.6
Daniel(config)#exit
Daniel#copy run start
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration
previously written by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...

[OK]
Daniel#
```

Nótese que en la configuración de la tabla de ruteo, todas las redes tienen como siguiente hop la dirección 192.168.28.6. que aún no se asigna. Sin embargo, al calcular el escenario, es fácil ver que esa dirección sólo puede ser asignada a la interfase de Sadrac que pertenece a la sub-red 192.168.28.4/30.

Un comando muy útil para revisar las tablas de ruteo es: desde modo privilegiado, **show ip route**

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

Gateway of last resort is not set

     192.168.28.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.28.16/28 is directly connected, Ethernet0
C       192.168.28.4/30 is directly connected, Serial0
```

Al inicio del desplegado se muestra lo que significa cada letra frente a cada entrada en la tabla de ruteo. Después, se muestra un enunciado que dice que no hay una ruta de último recurso, la ruta de último recurso muestra el siguiente hop al que se deben enviar los paquetes para los cuales no se encuentre una ruta en la tabla de ruteo (al no estar definida la ruta de último recurso, los paquetes para los cuales no haya siguiente salto, se destruyen.) Por último se muestra la red para la cual sí hay rutas definidas, sus sub-redes y la forma de llegar a cada una de esas sub-redes. En este caso sólo se muestran 2 sub-redes, las directamente conectadas a las interfases del ruteador, esto es por que la dirección a la que apuntan el resto de las sub-redes aún no se ha asignado.

En las demás configuraciones no se muestra el establecimiento de claves, sino directamente la configuración de las interfases y las tablas de ruteo.

```
Router(config)#hostname Sadrac
Sadrac(config)#int e0
Sadrac(config-if)#ip address 192.168.28.33 255.255.255.240
Sadrac(config-if)#desc conexion a la lan 192.168.28.32
Sadrac(config-if)#no shut
01:17:33 %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, changed state to up
01:17:33 %LINK-3-UPDOWN:  Interface Ethernet0, changed state to up

Sadrac(config-if)#int s1
Sadrac(config-if)#ip address 192.168.28.6 255.255.255.252
Sadrac(config-if)#desc conexion a Daniel
Sadrac(config-if)#no shutdown
01:19:17 %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed state to up
01:19:17 %LINK-3-UPDOWN:  Interface Serial1, changed state to up

Sadrac(config-if)#int s0
Sadrac(config-if)#ip address 192.168.28.9 255.255.255.252
Sadrac(config-if)#clock rate 64000
Sadrac(config-if)#desc conexion a Mesac
Sadrac(config-if)#no shut
01:20:51 %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to up
01:20:51 %LINK-3-UPDOWN:  Interface Serial0, changed state to up

Sadrac(config-if)#exit
Sadrac(config)#ip route 192.168.28.12 255.255.255.252 192.168.28.10
Sadrac(config)#ip route 192.168.28.16 255.255.255.240 192.168.28.5
Sadrac(config)#ip route 192.168.28.48 255.255.255.240 192.168.28.10
Sadrac(config)#ip route 192.168.28.64 255.255.255.240 192.168.28.10
Sadrac(config)#exit
Sadrac#
```

Puede ser que el teclear cada una de las entradas estáticas sea una labor bastante pesada, afortunadamente el ruteador cuenta con algunas combinaciones de tecleo para la edición. Véase la tabla 5.1

Secuencia	Acción del ruteador
Ctrl.+A	Mueve el cursor al inicio de la línea sin borrar
Ctrl.+B	Mueve el cursor un espacio atrás sin borrar
Ctrl.+D	Borra un caracter
Ctrl.+E	Mueve el cursor al final de la línea
Ctrl.+F	Mueve el cursor un espacio hacia adelante
Ctrl.+N	Despliega el siguiente en la historia de comandos introducidos
Ctrl.+P	Despliega el último comando introducido o el previo al reteclear
Ctrl.+R	Vuelve a desplegar una línea
Ctrl.+U	Borra una línea
Ctrl.+W	Borra una palabra
Ctrl.+Z	Regresa el cursor a modo privilegiado
Esc+B	Mueve el cursor una palabra hacia atrás sin borrar
Esc+F	Mueve el cursor una palabra hacia adelante
Flecha arriba	Despliega el último comando introducido o el previo al reteclear
Flecha abajo	Despliega el siguiente en la historia de comandos introducidos

Tabla 5.1 Secuencias de tecleo para edición.

Al pedir nuevamente la tabla de ruteo de Daniel, se observa que ésta ya tiene las entradas que apuntan hacia la dirección 192.168.28.6

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

Gateway of last resort is not set

     192.168.28.0/24 is variably subnetted, 7 subnets, 2 masks
C       192.168.28.16/28 is directly connected, Ethernet0
C       192.168.28.4/30 is directly connected, Serial0
S       192.168.28.64 [1/0] via 192.168.28.6
S       192.168.28.48 [1/0] via 192.168.28.6
S       192.168.28.32 [1/0] via 192.168.28.6
S       192.168.28.12 [1/0] via 192.168.28.6
S       192.168.28.8 [1/0] via 192.168.28.6
Daniel#
```

La configuración de Mesac:

```
Mesac(config)#Int e0
Mesac(config-if)#Ip address 192.168.28.49 255.255.255.240
Mesac(config-if)#desc conexion a la lan 192.168.28.48
Mesac(config-if)#no shut
00:51:00 %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, changed state to up
00:51:00 %LINK-3-UPDOWN: Interface Ethernet0, changed state to up

Mesac(config-if)#Int s1
Mesac(config-if)#Ip address 192.168.28.10 255.255.255.252
Mesac(config-if)#desc conexion a Sadrac
Mesac(config-if)#no shut
00:53:11 %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed state to up
00:53:11 %LINK-3-UPDOWN: Interface Serial1, changed state to up

Mesac(config-if)#Int s0
Mesac(config-if)#Ip address 192.168.28.13 255.255.255.252
Mesac(config-if)#clock rate 64000
Mesac(config-if)#desc conexion a Abed-nego
Mesac(config-if)#no shut
00:54:53 %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to up
00:54:53 %LINK-3-UPDOWN: Interface Serial0, changed state to up

Mesac(config-if)#exit
Mesac(config)#Ip route 192.168.28.4 255.255.255.252 192.168.28.9
Mesac(config)#Ip route 192.168.28.16 255.255.255.240 192.168.28.9
Mesac(config)#Ip route 192.168.28.32 255.255.255.240 192.168.28.9
Mesac(config)#Ip route 192.168.28.64 255.255.255.240 192.168.28.14
Mesac(config)#
```

La configuración de Abed-nego:

```
Abed-nego(config)#Int e0
Abed-nego(config-if)#Ip address 192.168.28.65 255.255.255.240
Abed-nego(config-if)#desc conexion a la lan 192.168.28.64
Abed-nego(config-if)#no shut
01:02:18 %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, changed state to up
01:02:18 %LINK-3-UPDOWN: Interface Ethernet0, changed state to up

Abed-nego(config-if)#Int s1
Abed-nego(config-if)#Ip address 192.168.28.14 255.255.255.252
Abed-nego(config-if)#desc conexion a Mesac
```

```
Abed-nego(config-if)#no shut
01:04:29 %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed state to up
01:04:29 %LINK-3-UPDOWN:  Interface Serial1, changed state to up

Abed-nego(config-if)#
```

Ya que todas las interfases a las que se hace referencia en las tablas de ruteo se han establecido, es buen momento de ver las tablas de ruteo de los ruteadores.

```
Daniel#show ip route
        192.168.28.0/24 is variably subnetted, 7 subnets, 2 masks
C         192.168.28.16/28 is directly connected, Ethernet0
C         192.168.28.4/30 is directly connected, Serial0
S         192.168.28.64 [1/0] via 192.168.28.6
S         192.168.28.48 [1/0] via 192.168.28.6
S         192.168.28.32 [1/0] via 192.168.28.6
S         192.168.28.12 [1/0] via 192.168.28.6
S         192.168.28.8 [1/0] via 192.168.28.6
Daniel#

Sadrac#show ip route
        192.168.28.0/24 is variably subnetted, 7 subnets, 2 masks
C         192.168.28.32/28 is directly connected, Ethernet0
C         192.168.28.4/30 is directly connected, Serial1
C         192.168.28.8/30 is directly connected, Serial0
S         192.168.28.64 [1/0] via 192.168.28.10
S         192.168.28.48 [1/0] via 192.168.28.10
S         192.168.28.16 [1/0] via 192.168.28.5
S         192.168.28.12 [1/0] via 192.168.28.10
Sadrac#

Mesac#show ip route
        192.168.28.0/24 is variably subnetted, 7 subnets, 2 masks
C         192.168.28.48/28 is directly connected, Ethernet0
C         192.168.28.8/30 is directly connected, Serial1
C         192.168.28.12/30 is directly connected, Serial0
S         192.168.28.64 [1/0] via 192.168.28.14
S         192.168.28.32 [1/0] via 192.168.28.9
S         192.168.28.16 [1/0] via 192.168.28.9
S         192.168.28.4 [1/0] via 192.168.28.9
Mesac#
```

```
Abed-nego#show ip route
        192.168.28.0/24 is variably subnetted, 7 subnets, 2 masks
C          192.168.28.64/28 is directly connected, Ethernet0
C          192.168.28.8/30 is directly connected, Serial1
S          192.168.28.48 [1/0] via 192.168.28.13
S          192.168.28.32 [1/0] via 192.168.28.13
S          192.168.28.16 [1/0] via 192.168.28.13
S          192.168.28.8 [1/0] via 192.168.28.13
S          192.168.28.4 [1/0] via 192.168.28.13
Abed-nego#
```

En cada caso se cortó el desplegado dado por el ruteador para ahorrar espacio. Sin embargo, se puede ver que las entradas de cada tabla de ruteo están catalogadas como c ó s, en donde c significa directamente conectada y s significa establecida por medio de ruteo estático.

La conectividad de los *hosts* debe probarse, pero en cuanto a los ruteadores no hay problemas de conectividad.

A modo de ejemplo se hacen algunas pruebas de conectividad:

```
Daniel>ping 192.168.28.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.28.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/9/9 ms

Daniel>ping 192.168.28.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.28.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/9/9 ms

Daniel>ping 192.168.28.65
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.28.65, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/9/9 ms

Daniel>ping 192.168.28.49
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.28.6, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/9/9 ms
```

El comando ping se puede introducir desde el modo usuario normal y desde el modo privilegiado (aunque con algunas diferencias), cuando el ping tiene éxito el ruteador despliega signos de admiración.

Los primeros *hosts* en cada red LAN son: 192.168.28.18, 192.168.28.34, 192.168.28.50 y 192.168.28.66. un buen ejercicio es calcular el rango de *hosts* en cada LAN.

5.4 Ruteo de Último Recurso

El ruteo de último recurso permite al ruteador saber que hacer con los paquetes destinados a redes para las cuales no hay entrada en la tabla de ruteo. Para el examen de Cisco, el ruteo de último recurso o *Default routing* se utiliza tan sólo en ruteadores que tienen una sola salida para todas sus redes directamente conectadas. En el ejemplo de los príncipes de Judá, escenario 5.2, todas las rutas estáticas que se dieron de alta en el ruteador Daniel tienen una y la misma interfase como siguiente salto. La misma situación se tiene con las rutas en la tabla de ruteo del ruteador Abed-nego.

La configuración la las tablas de ruteo de Daniel, así como la de Abed-nego, se pueden hacer por medio de ruteo de último recurso en vez de hacerse por ruteo estático. Hay sólo dos comandos necesarios para implementar el ruteo de último recurso: **ip route 0.0.0.0 0.0.0.0 [vía de salida]** y el comando **ip classless**.

El primer comando especifica que para llegar a cualquier red con cualquier máscara se debe seguir la vía de salida indicada. Y el segundo comando, **ip classless**, le dice al ruteador que las redes que se utilizan no son *classfull*, es decir no utilizan la máscara por *default*. Al decir cualquier IP con cualquier máscara definitivamente se habla de cualquier máscara, no solo las máscaras por *default* por clase.

La configuración alterna (en lugar de hacerla por ruteo estático) para las tablas de ruteo de Daniel y de Abed-nego se muestra a continuación:

```
Daniel(config-if)#exit
Daniel(config)#ip route 0.0.0.0 0.0.0.0 192.168.28.6
Daniel(config)#ip classless

Abed-nego(config-if)#exit
Abed-nego(config)#ip route 0.0.0.0 0.0.0.0 192.168.28.13
Abed-nego(config)#ip classless
```

Es importante recalcar que esta configuración no es posible en cualquier ruteador sino solamente en aquellos en los cuales todas las entradas a la tabla de ruteo se dirigen a la misma interfase (por supuesto que esto no incluye a las redes directamente conectadas.)

La tabla de ruteo de Daniel es:

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

Gateway of last resort is 192.168.28.6 to network 0.0.0.0

     192.168.28.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.28.16/28 is directly connected, Ethernet0
C       192.168.28.4/30 is directly connected, Serial0
S*   0.0.0.0 [1/0] via 192.168.28.6
Daniel#
```

Se puede ver que la única entrada en la tabla de ruteo, además de las redes directamente conectadas, es la de la ruta de último recurso. Además el enunciado sobre la tabla de ruteo dice que sí hay una puerta de salida de último recurso y que ésta es 192.168.28.6. cualquier paquete que no esté destinado para las redes locales del ruteador se enviará a esa interfase.

Nótese que la letra frente a la entrada en la tabla de ruteo es "S*" lo cual significa que esa entrada es una ruta de último recurso.

```
Daniel#ping 192.168.28.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.28.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/9/9 ms

Daniel#ping 192.168.28.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.28.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/9/9 ms
```

```
Daniel#ping 192.168.28.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.28.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/9/9 ms

Daniel#ping 192.168.28.64
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.28.64, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/9/9 ms
```

Por supuesto, sí hay conectividad.

5.5 Ruteo Dinámico

En el ruteo dinámico hay protocolos de ruteo que se encargan de hacer todo el trabajo de buscar y establecer las rutas a las diferentes redes en las tablas de ruteo de cada ruteador. Después de haber visto el trabajo y la probabilidad de errores que el ruteo estático significa, se puede apreciar la bondad del ruteo dinámico. Sin embargo, hay que tener en cuenta que la comodidad siempre cuesta y en este caso el costo es tiempo de procesador y ancho de banda.

Hay varios protocolos de ruteo, y es posible utilizar más de uno al mismo tiempo en el mismo ruteador. Esto podría ser causa de errores y confusión pero no lo es, gracias en gran parte a la distancia administrativa. La distancia administrativa es un número comprendido entre el 0 y el 255 y que se asocia a cada uno de los protocolos de ruteo. El ruteador le da prioridad a las rutas adquiridas por protocolos cuya distancia administrativa es menor.

Algunos protocolos con sus distancias administrativas por *default* se muestran en la tabla 5.2

Protocolo	Distancia administrativa
Interfases directamente conectadas y rutas estaticas especificando la propia interfase	0
Rutas estaticas especificando el proximo salto	1
EIGRP (Enhanced Interior Gateway Routing Protocol)	90
IGRP (Interior Gateway Routing Protocol)	100
OSPF (Open Shortest Path First)	110
RIP (Routing Information Protocol)	120
Sin entrada en la tabla de ruteo	255

Tabla 5.2 Distancias administrativas

Por ejemplo, si en un ruteador se utiliza RIP como protocolo de ruteo, y RIP descubre una ruta para llegar a cierta red, pero además se introduce una ruta estática para llegar a la misma red, entonces el ruteador se basará en la distancia administrativa de los métodos por los cuales fue introducida la entrada en la tabla de ruteo para determinar la ruta que utilizará. En este ejemplo, la entrada estática tiene una distancia administrativa de 1 mientras que la ruta por RIP tiene una distancia administrativa de 120. El ruteador no le hará caso a la ruta obtenida por RIP.

Los protocolos de ruteo dinámico pueden ser basados en dos métodos: vector de distancia (*distance vector*) o estado de liga (*link state.*)

Los protocolos de vector de distancia son RIP e IGRP. OSPF se basa en link state y EIGRP es un protocolo híbrido, es decir se basa en distance vector y en link state.

En los protocolos de vector de distancia, cada ruteador manda, a intervalos periódicos, la información contenida en sus tablas de ruteo a los ruteadores directamente conectados a él, y éstos a su vez mandan la información de sus tablas a los ruteadores directamente conectados a ellos y así sucesivamente. Este método se conoce como compartir por rumor.

Cuando todas las tablas de ruteo en la red tienen la misma información entonces se dice que hay convergencia. Dada la manera en que los ruteadores comparten información, los protocolos de vector de distancia tienen una convergencia bastante lenta a comparación de otros protocolos.

Los protocolos de vector de distancia se basan en la distancia esquemática, es decir en la cuenta de hops, para determinar el mejor camino para un paquete.

OSPF que es un protocolo de link state, manda un paquete con la información de las redes directamente conectadas a él a cada uno de los ruteadores en la red. Esto lo hace al inicializarse (prenderse) o cuando hay un cambio en las redes conectadas a él que afecten el ruteo. Por esto, los protocolos de link state son más rápidos para converger. Al no mandar paquetes con información aprendida pero no comprobada, link state es mucho menos susceptible a la propagación de errores de ruteo en la red. Además, como no se envían paquetes a intervalos regulares sino solo para reflejar cambios, link state tiene un costo en ancho de banda mucho menor que distance vector. Link state utiliza tres tablas de ruteo y varios parámetros, principalmente ancho de banda, para determinar la mejor ruta hacia una red.

5.5.1 RIP

RIP es un protocolo de vector de distancia, es decir que entre otras características se basa en la cuenta de hops como su métrica para determinar la mejor ruta y comparte la información de sus tablas de ruteo por medio de rumores.

El compartir la información por medio de rumores tiene un problema:

Supóngase que los ruteadores en la figura 5.4 han sido configurados con RIP y ya han convergido.

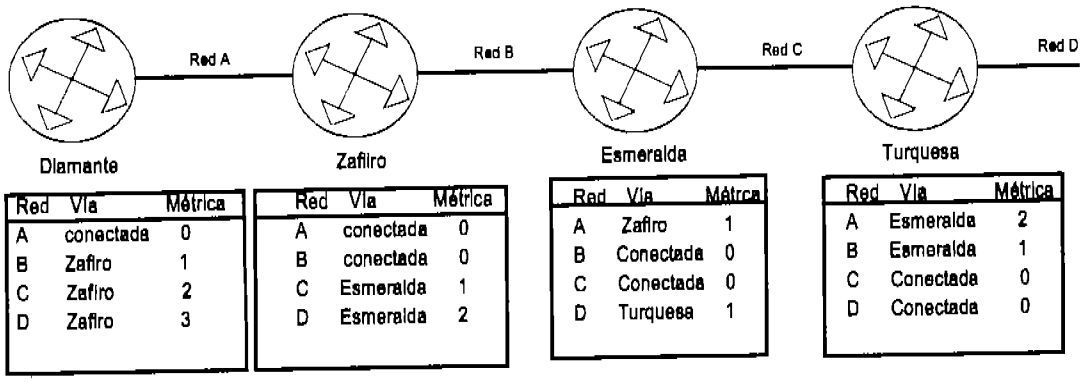


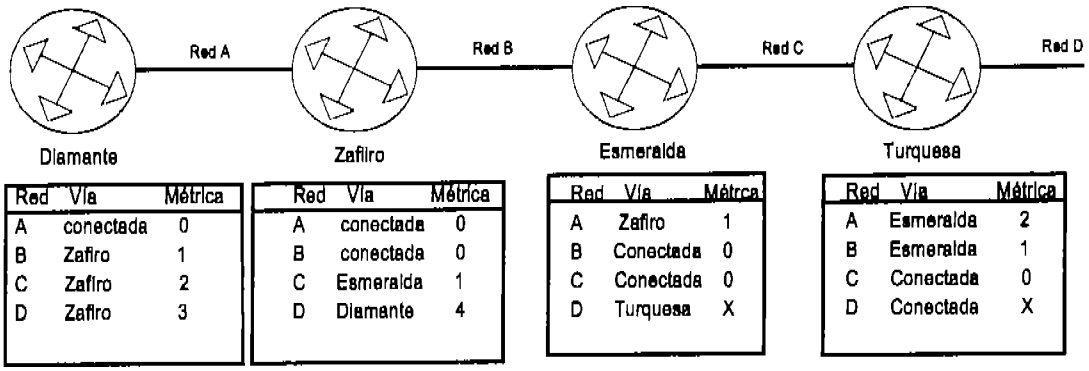
Figura 5.4 Ruteadores configurados por RIP y sus tablas de ruteo

Sin embargo, de repente la red D tiene un problema por el cual queda inaccesible. La próxima convergencia podría ser así con respecto a la red D:

- Turquesa marca como inaccesible la red D en su tabla de ruteo y al llegar su periodo de mandar el rumor envía a esmeralda la información en su tabla.
- Esmeralda recibe la información de la tabla de ruteo de Turquesa y al ver que la red D a la que antes podía accesar por medio de Turquesa es inaccesible para Turquesa, la marca como inaccesible en su propia tabla. Llegado el momento de mandar el rumor a los ruteadores directamente conectados, lo hace.
- Zafiro recibe la tabla de Esmeralda y ve que Esmeralda que era su salida para la red D no sabe que hacer con ese paquete, así que marca a D como inaccesible. Sin embargo, ya ha pasado mucho tiempo y el momento de que Diamante mande su rumor llega antes que el de Zafiro, así que Zafiro recibe la tabla proveniente de Diamante. En esta tabla dice claramente que Diamante sí tiene una ruta definida para llegar a D, así que, Zafiro actualiza su tabla quitando a Esmeralda que no sabe que hacer con paquetes con destino en D y poniendo a Diamante que sí sabe.

¡Ya se ve venir el problema! Zafiro tiene a Diamante como salida para llegar a D y Diamante tiene a Zafiro como salida para llegar a D.

Las tablas de ruteo después de ese rumor (más bien chisme) quedan como se muestra en la figura 5.5



Red	Vía	Métrica
A	conectada	0
B	Zafiro	1
C	Zafiro	2
D	Zafiro	3

Red	Vía	Métrica
A	conectada	0
B	conectada	0
C	Esmeralda	1
D	Diamante	4

Red	Vía	Métrica
A	Zafiro	1
B	Conectada	0
C	Conectada	0
D	Turquesa	X

Red	Vía	Métrica
A	Esmeralda	2
B	Esmeralda	1
C	Conectada	0
D	Conectada	X

Figura 5.5 Tablas de ruteo después del "chisme"

Al siguiente rumor de Zafiro, Diamante actualizará su métrica a 5, y al siguiente rumor de Diamante, Zafiro lo hará a 6, y así sucesivamente hacia infinito de modo que nunca habrá una convergencia en esta red.

Afortunadamente, los protocolos de vector de distancia tienen una cuenta máxima de hops. En el caso de RIP ésta es de 15, es decir que un ruteador que está configurado por medio de RIP, tan sólo verá las redes con métrica de 15 o menos. En otras palabras habrá 16 mensajes de rumor entre Zafiro y diamante, y entonces la red D se declarará como inaccesible. Por supuesto que esto es un avance si consideramos la cuenta hacia infinito, pero aún así no parece muy eficiente. Y no lo es.

Además de la cuenta máxima de hops, los protocolos de vector de distancia cuentan con un par de técnicas para eliminar la cuenta hacia el infinito: Split horizon y Poison reverse.

Split horizon previene la formación de ciclos por medio de una regla muy sencilla: un ruteador no puede publicar la información que aprendió a través de una interfase por esa misma interfase. Al utilizar split horizon, Diamante no puede publicar la información que recibió acerca de la red D ya que la única interfase que tiene activa es por la cual aprendió esa ruta.

Poison reverse consiste en que el ruteador que tiene directamente conectada una red que deja de ser accesible, comienza un "envenenamiento" de todas las entradas hacia esa red. Al determinar que la red D es inaccesible, el ruteador Turquesa publica esa red como una red a distancia 16. RIP tiene una cuenta máxima de saltos de 15 así que lo que está haciendo Turquesa es sacar la red D del alcance de Zafiro, Zafiro a su vez marca como inalcanzable la red D y publica que la red es inalcanzable y así sucesivamente dejando la ruta en las tablas de ruteo (por el momento) pero marcándola como inalcanzable.

Un problema más que los protocolos de vector de distancia deben resolver es el flapping. El flapping se presenta cuando una red tiene una conexión en falso o por alguna otra razón queda inaccesible y de inmediato accesible y nuevamente inaccesible y fluctúa velozmente entre estos dos estados. Dado que los cambios que

se presentan con dicha red son mucho más rápidos que el tiempo de convergencia, las redes con ese problema prácticamente nunca convergen. La solución es bastante sencilla: para que una ruta se declare inaccesible, ésta tiene que haber estado inaccesible por un periodo predeterminado de tiempo de espera, y para que una red que está abajo se declare nuevamente arriba, ésta tiene que haber estado arriba por lo menos el periodo de tiempo predeterminado. A este periodo de tiempo de histéresis se le llama *Holddown*. Si, por ejemplo, una ruta se cae pero durante el tiempo de holddown llega una ruta hacia la misma red pero con una métrica igual o peor que la que se tenía, la ruta nueva no se instala en la tabla de ruteo, dando oportunidad a que la ruta instalada se estabilice antes de ser cambiada. Sin embargo, si durante el tiempo de holddown, llega una ruta con mejor métrica, ésta se instala de inmediato.

En RIP, el holddown por *default* es de 180 segundos.

El manejo de los cronómetros en los protocolos de vector de distancia es muy importante, y normalmente, la mejor manera de manejarlos es dejarlos en sus valores de fábrica. Además del holddown, hay tres valores de tiempo a considerar para RIP: El periodo para enviar un rumor con actualizaciones (*update*) de RIP es de 30 segundos, el periodo para declarar una red como inválida es de 180 segundos y el periodo para eliminar una ruta de la tabla de ruteo (*flush*) es de 240 segundos.

5.5.2 Configuración de RIP

En vez de configurar rutas estáticas, dejar que el ruteador pueble la tabla de ruteo, ¡Suena como una muy buena idea!

A diferencia de la configuración de las rutas estáticas en donde se le decía al ruteador cómo llegar a las rutas que no veía, en el ruteo por RIP, se le dice al ruteador cuáles de las redes que ve, debe publicar para que los demás ruteadores las vean.

RIP es un protocolo *classfull*, es decir, no envía información de la máscara de las redes que publica. Esto significa que RIP no soporta VLSM. (La segunda versión de RIP sí soporta VLSM, pero RIPv2 no es tema del examen)

Al publicar sus redes, RIP simplemente las publica con su máscara por clase.

El comando para habilitar el uso de RIP en el ruteador es, desde el modo de configuración global, **router rip** y para publicar las redes directamente conectadas a él que se incluirán en el rumor se utliliza el comando **network**:

```
Router(config)#router rip
Router(config-router)#network 10.0.0.0
```

Nótese que la red se especificó como un identificador de la clase a la que pertenece.

Escenario 5.3

Considerando que los ruteadores en la figura 5.6 ya han sido configurados a excepción de las tablas de ruteo, configurar éstas por medio de RIP para proveer conectividad total a la red. (El escenario en sí, presenta una buena oportunidad para practicar *subnetting*)

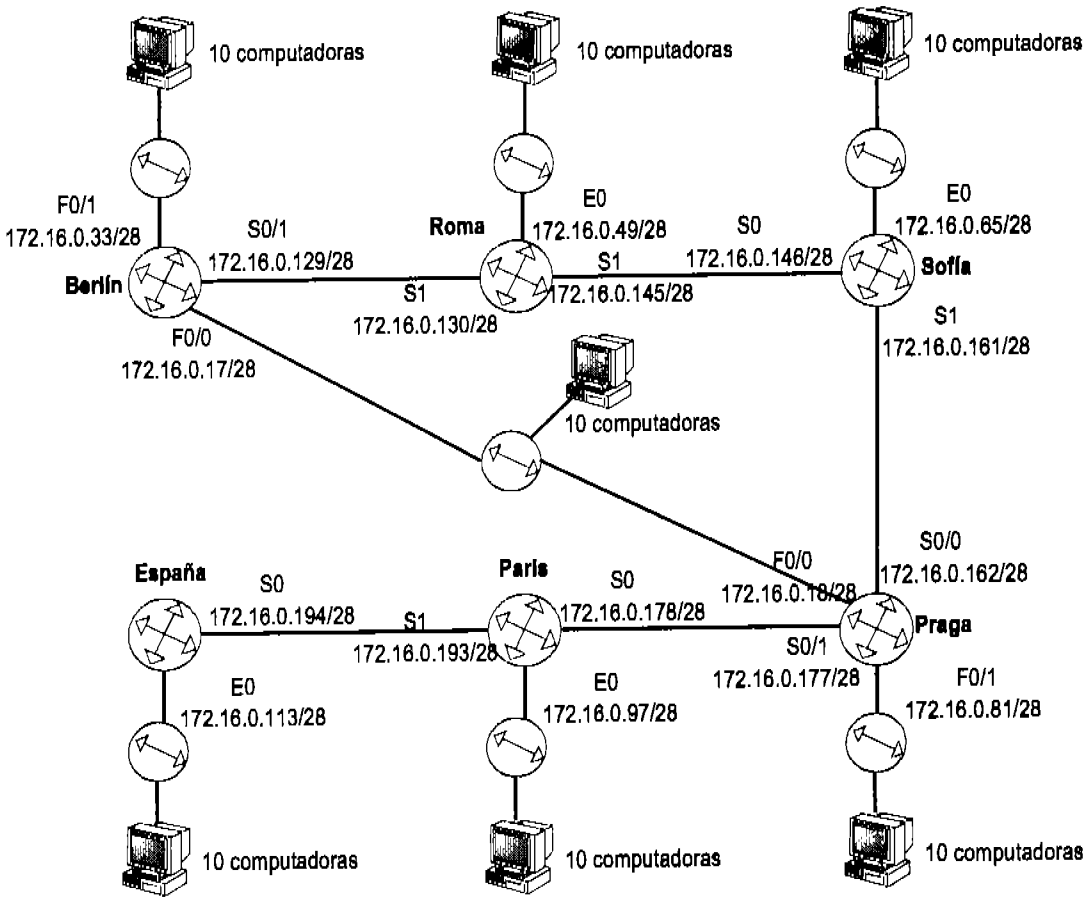


Figura 5.6 Escenario para configurar RIP.

Ya se espera que la configuración de las tablas por medio de RIP sea más fácil que por medio de ruteo estático, pero tal vez sea aún más fácil de lo que se espera:

```
Berlin(config)#router rip
Berlin(config-router)#network 172.16.0.0

Roma(config)#router rip
Roma(config-router)#network 172.16.0.0

Sofia(config)#router rip
sofia(config-router)#network 172.16.0.0
```

```
Praga(config)#router rip
Praga(config-router)#network 172.16.0.0

Paris(config)#router rip
Paris(config-router)#network 172.16.0.0

Espana(config)#router rip
Espana(config-router)#network 172.16.0.0
```

¡Tablas configuradas!

Al pedir la tabla de ruteo de Berlín se tiene:

```
Berlin#show ip route
```

(Se omitió la lista de códigos)

```
R       172.16.0.192 [120/3] via 172.16.0.18. 00:00:27. FastEthernet0/0
R       172.16.0.176 [120/2] via 172.16.0.18. 00:00:13. FastEthernet0/0
R       172.16.0.160 [120/2] via 172.16.0.130. 00:00:13. Serial0/1
R       172.16.0.144 [120/1] via 172.16.0.130. 00:00:9. Serial0/1
C       172.16.0.128 is directly connected. Serial0/1
R       172.16.0.112 [120/4] via 172.16.0.18. 00:00:29. FastEthernet0/0
R       172.16.0.96 [120/3] via 172.16.0.18. 00:00:26. FastEthernet0/0
R       172.16.0.80 [120/2] via 172.16.0.18. 00:00:13. FastEthernet0/0
R       172.16.0.64 [120/2] via 172.16.0.130. 00:00:13. Serial0/1
R       172.16.0.48 [120/1] via 172.16.0.130. 00:00:9. Serial0/1
C       172.16.0.32 is directly connected. FastEthernet0/1
C       172.16.0.16 is directly connected. FastEthernet0/0
```

Dado que todas las rutas pertenecen a la misma red por clase, las doce rutas del escenario se han dado de alta con un par de comandos.

Nótese que antes de cada ruta aparece la forma en que se adquirió la misma: C-las directamente conectadas y R-las descubiertas por RIP. Después de la letra, se enlista la red de destino y, entre corchetes, la distancia administrativa de RIP (120) sobre la métrica hasta el destino (cuenta de hops.) Después aparece el tiempo de entrega y por último la interfase propia de salida.

Nótese también, que al haber dos rutas para llegar al mismo destino, RIP eligió la más corta en saltos para cada caso.

Si desde Berlín se da el comando **Traceroute** que es el equivalente en ruteadores a Tracert en PC's, para ver el camino que siguen los paquetes para llegar a un *host* de la red de España, se ve:

```
Berlin#traceroute 172.16.0.120
Type escape sequence to abort.
Tracing the route to 172.16.0.120

1 172.16.0.18 255.255.255.240 28 msec * 28 msec
2 172.16.0.178 255.255.255.240 28 msec * 28 msec
3 172.16.0.194 255.255.255.240 28 msec * 28 msec
4  28 msec * 28 msec
```

Hay cuatro saltos desde el ruteador Berlín hasta cualquier computadora en la LAN de España, RIP detectó que la ruta más corta es: Berlín – Praga – Paris – España – *Host* 172.16.0.120.

Pero ¿Qué pasa si se desconecta un cable sobre la mejor ruta? Véase la figura 5.7.

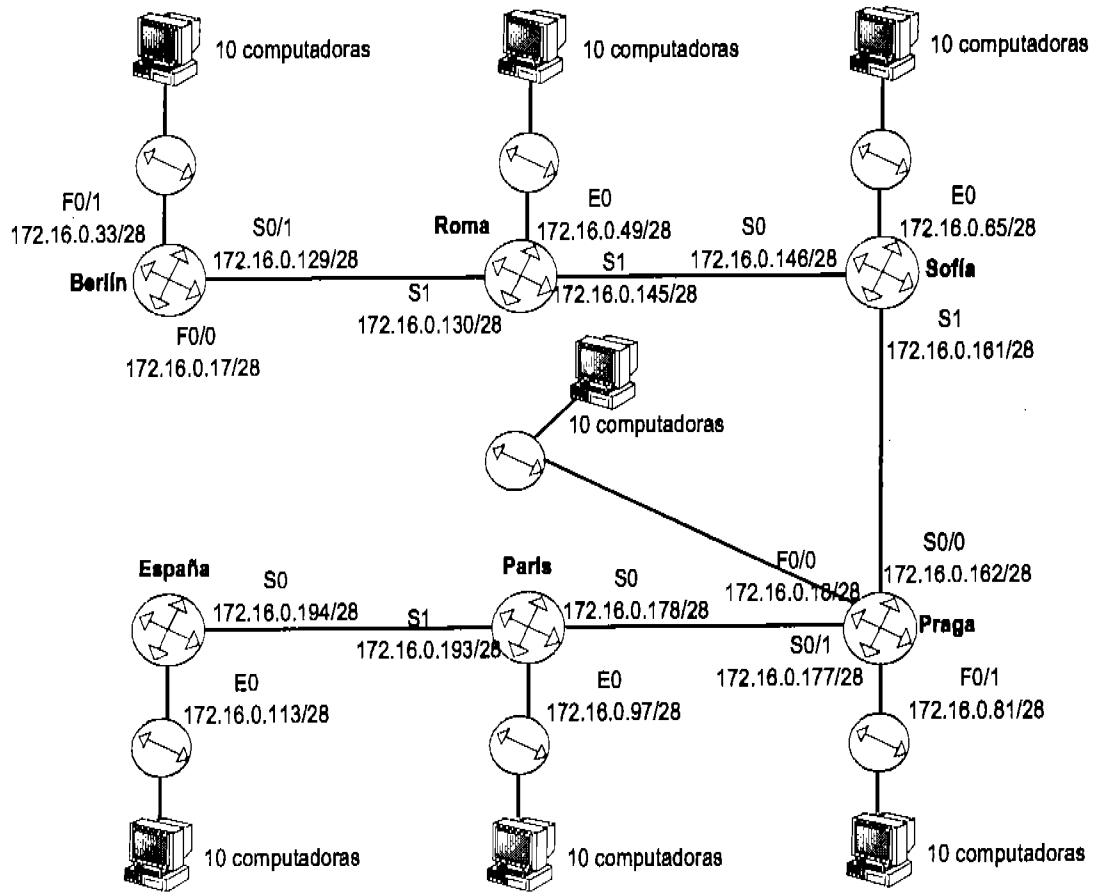


Figura 5.7 Análisis de RIP al desconectar una ruta.

Después de desconectar el cable *Ethernet* que conectaba a Berlín con la red 16 y esperar unos momentos a que la red converja, la tabla de ruteo de Berlín se ve así:

```
Berlin#show ip route

(Se omitió la lista de códigos)

R       172.16.0.192 [120/4] via 172.16.0.130. 00:00:9. Serial0/1
R       172.16.0.176 [120/3] via 172.16.0.130. 00:00:9. Serial0/1
R       172.16.0.160 [120/2] via 172.16.0.130. 00:00:13. Serial0/1
R       172.16.0.144 [120/1] via 172.16.0.130. 00:00:9. Serial0/1
C       172.16.0.128 is directly connected. Serial0/1
R       172.16.0.112 [120/5] via 172.16.0.130. 00:00:9. Serial0/1
R       172.16.0.96 [120/4] via 172.16.0.130. 00:00:9. Serial0/1
R       172.16.0.80 [120/3] via 172.16.0.130. 00:00:13. Serial0/1
R       172.16.0.64 [120/2] via 172.16.0.130. 00:00:13. Serial0/1
R       172.16.0.48 [120/1] via 172.16.0.130. 00:00:9. Serial0/1
C       172.16.0.32 is directly connected. FastEthernet0/1
R       172.16.0.16[120/3] via 172.16.0.130. 00:00:13. Serial0/1
```

La tabla se actualizó sin necesidad de ingresar comando alguno. Gracias a que el ruteo de esta red es dinámico y que hay rutas redundantes, al conectividad en la misma no se perdió.

Al pedir un Traceroute (recuérdese que *Tracert* no es un comando válido para IOS) desde el ruteador Berlín al *host* 172.16.0.120:

```
Berlin#traceroute 172.16.0.120
Type escape sequence to abort.
Tracing the route to 172.16.0.120

1 172.16.0.130 255.255.255.240 28 msec * 28 msec
2 172.16.0.146 255.255.255.240 28 msec * 28 msec
3 172.16.0.162 255.255.255.240 28 msec * 28 msec
4 172.16.0.178 255.255.255.240 28 msec * 28 msec
5 172.16.0.194 255.255.255.240 28 msec * 28 msec
6  28 msec * 28 msec
```

Una ruta larga es mejor que ninguna ruta.

Hay ocasiones en que se requiere que la propagación del rumor de RIP no alcance ciertas secciones de la red. El comando passive-interface permite especificar una interfase por la cual no se transmitan rumores, pero que sí los reciba.

Escenario 5.4

Un ruteador modelo 2522 (este modelo tiene 10 interfases seriales y una *Ethernet*) tiene las siguientes redes conectadas directamente:

S0- 170.45.23.0/28
S1- 195.12.12.96/28
S2- 19.35.23.80/28
S3- 19.5.7.123/28
S4- 170.45.9.224/28
S5- 195.12.13.112/28
S6- 195.12.12.112/28
S7- 19.23.45.208/28
S8- 170.46.56.144/28
S9- 195.12.12.160/28
E0- 170.45.95.32/28

(Como ejercicio adicional se puede comprobar que las direcciones dadas, en efecto son direcciones válidas para redes.) Se desea configurar RIP en este ruteador pero evitar que la interfase serial 7 propague cualquier información obtenida por RIP. Sin embargo, todas las interfases (incluyendo S7) deben poder recibir la información RIP de otros ruteadores.

Para configurar este ruteador tan sólo es necesario llegar a modo de configuración global y teclear los siguientes comandos:

```
Router(config)#router rip
Router(config-router)#network 19.0.0.0
Router(config-router)#network 170.45.0.0
Router(config-router)#network 170.46.0.0
Router(config-router)#network 195.12.12.0
Router(config-router)#network 195.12.13.0
Router(config-router)#passive-interface serial 7
Router(config-router)#exit
```

5.5.3 IGRP (*Interior Gateway Routing Protocol*)

IGRP es un protocolo propiedad de Cisco (a pesar de esto no se requiere un conocimiento profundo de IGRP para el examen.) Como es propiedad de Cisco, IGRP sólo funciona en ruteadores Cisco.

IGRP también es un protocolo de vector de distancia pero sus cronómetros y parámetros son algo diferentes a los de RIP. Para comenzar, la métrica de IGRP, que se conoce como métrica compuesta, se basa en el ancho de banda y retardo en la línea (*composite metric= bandwidth + delay*), aunque es posible configurar otros parámetros más para determinar la mejor ruta (MTU, confiabilidad y carga.) Además de permitir una métrica más sofisticada, IGRP tiene otras dos ventajas sobre RIP: la cuenta máxima de saltos de IGRP es de 255 (¡ya no más redes pequeñas!) y el manejo de sistemas autónomos.

El sistema autónomo (AS) es un identificador numérico comprendido entre 1 y 65535. Este número sirve para agrupar los ruteadores de manera que todos aquellos con el mismo sistema autónomo se comuniquen entre sí sus tablas de ruteo, pero no lo hagan con otros ruteadores que no sean miembros del mismo AS. Un ruteador puede pertenecer a tantos sistemas autónomos como sea necesario.

Configurar de manera básica IGRP es muy similar a como se configura RIP, con la excepción del AS. Los comandos para configurar IGRP son **router igrp [AS]** y, al igual que en RIP, **network** seguido de la red por clase a publicar.

```
Router(config)#router igrp 10
Router(config-router)#network 172.16.0.0
```

Es importante recordar que tanto RIP como IGRP son *classfull*.

Si a los ruteadores configurados en el escenario 5.3 se les agregan las siguientes instrucciones:

```
Berlin(config)#router igrp 1
Berlin(config-router)#network 172.16.0.0

Roma(config)#router igrp 1
Roma(config-router)#network 172.16.0.0

Sofia(config)#router igrp 1
sofia(config-router)#network 172.16.0.0

Praga(config)#router igrp 1
Praga(config-router)#network 172.16.0.0

Paris(config)#router igrp 1
Paris(config-router)#network 172.16.0.0

Espana(config)#router igrp 1
Espana(config-router)#network 172.16.0.0
```

Se habrá configurado IGRP en ellos. Nótese que los sistemas autónomos en todos los ruteadores son iguales.

A propósito no se borró RIP de los ruteadores por lo que ambos protocolos están funcionando en cada uno de los ruteadores.

La tabla de ruteo de Berlín, con ambos protocolos de ruteo activos se ve así:

```
Berlin#show ip route

(Se omitió la lista de códigos)

I       172.16.0.192 [100/153512] via 172.16.0.18. 00:00:27. FastEthernet0/0
I       172.16.0.176 [100/150624] via 172.16.0.18. 00:00:13. FastEthernet0/0
I       172.16.0.160 [100/140230] via 172.16.0.130. 00:00:13. Serial0/1
I       172.16.0.144 [100/140789] via 172.16.0.130. 00:00:9. Serial0/1
C       172.16.0.128 is directly connected. Serial0/1
I       172.16.0.112 [100/173604] via 172.16.0.18. 00:00:29. FastEthernet0/0
I       172.16.0.96 [100/158754] via 172.16.0.18. 00:00:26. FastEthernet0/0
I       172.16.0.80 [100/153925] via 172.16.0.18. 00:00:13. FastEthernet0/0
I       172.16.0.64 [100/153706] via 172.16.0.130. 00:00:13. Serial0/1
I       172.16.0.48 [100/140034] via 172.16.0.130. 00:00:9. Serial0/1
C       172.16.0.32 is directly connected. FastEthernet0/1
C       172.16.0.16 is directly connected. FastEthernet0/0
```

La letra I del desplegado anterior quiere decir que la entrada fue descubierta por IGRP y el número entre corchetes es la distancia administrativa sobre la métrica compuesta. Entre más baja sea la métrica compuesta, mejor será la ruta para IGRP.

Pero... ¿Dónde esta RIP? – RIP está funcionando, pero ninguno de sus descubrimientos logra ingresar a la tabla de ruteo. La razón de esto es la distancia administrativa. Recuérdese que la distancia administrativa de RIP es 120 mientras que la de IGRP es 100. RIP sigue allí y sigue consumiendo ancho de banda, RAM y tiempo de procesador: los recursos más valiosos con que cuenta un ruteador. A menos que se tengan razones poderosas para dejarlo allí, como podría ser tener redundancia de protocolos, al configurar IGRP, RIP se debe deshabilitar.

Para deshabilitar RIP se utiliza:

```
router(config)#no router rip
```

Los cronómetros de IGRP tienen tiempos diferentes a los de RIP: El update es de 90 segundos por *default*, el tiempo de invalidez es de tres veces el update, el hoddown es de tres veces el update más diez segundos y el flush es siete veces el update.

Se recomienda explorar el comando **debug** desde modo privilegiado, para cada uno de los protocolos de ruteo vistos. Este comando provee abundante información en tiempo real sobre la emisión y recepción de paquetes de información de rutas que los protocolos de ruteo intercambian.

Capítulo 6

Herramientas de Conectividad

6.1 Introducción

En este capítulo se tratan algunas de las herramientas más importantes en el manejo y monitoreo de las redes Cisco. Normalmente, el monitoreo y manejo de una red tiene más que ver con anticipar y resolver problemas qué con llevar estadísticas o implementar mejoras. De cualquier manera, un administrador de red será más útil mientras más herramientas de manejo de su red domine.

6.2 El Registro de Configuración

El registro de configuración es un conjunto de 16 *bit*s que se guarda en la memoria NVRAM de todos los ruteadores Cisco e indica al ruteador la forma en que debe arrancar. Este registro puede ser modificado por el administrador y hacer que el ruteador deje de arrancar (lo he visto varias veces) o para resolver problemas tan graves como el extravío de la palabra clave de acceso. La figura 6.1 muestra el registro de configuración y el significado de cada *bit*.

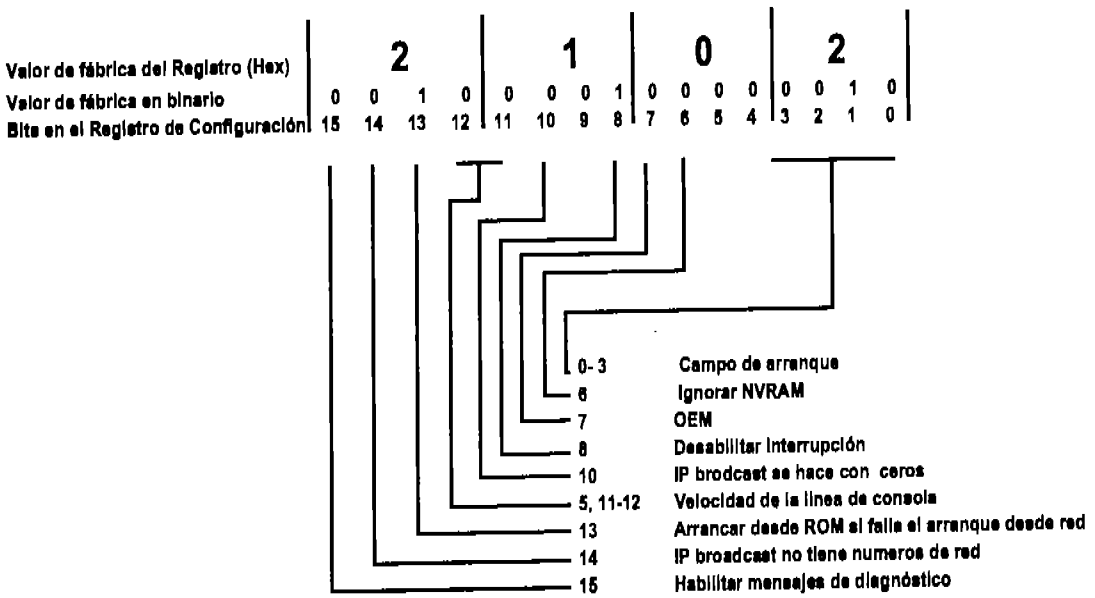


Figura 6.1 Registro de configuración

En la figura 6.1 se muestra que los *bit*s del registro de configuración van del 0 al 15 (Cisco normalmente comienza sus conteos desde cero) y cómo al modificar el valor de un solo *bit* puede cambiar por completo la forma en que el ruteador arranca. Los valores de fábrica del registro tan sólo tienen tres *bit*s encendidos: los *bit*s número 13, 8 y 1. Lo que significa que el ruteador debe arrancar utilizando los comandos de booteo especificados en la NVRAM, el ruteador además, debe buscar un archivo de arranque desde red y arrancar desde ROM si esto falla, y la interrupción del proceso

de arranque está habilitada. El campo de arranque conformado por los *bit*s 0 al 3 tiene diferentes significados según el número en hexadecimal que representen:

0- Dice al ruteador que debe arrancar en modo ROM. El ROM monitor (*rommon*) utiliza un pequeño IOS llamado mini IOS para cargar el IOS y realizar algunas funciones muy básicas de configuración. (Algo así como utilizar el DOS en una PC)

1- Hace que el ruteador arranque utilizando una imagen del IOS almacenada en ROM.

2 a F- Dice al ruteador que debe arrancar utilizando los comandos de booteo almacenados en RAM.

El comando **show version** muestra, entre otras cosas, el estado actual del registro de configuración:

```
Router>show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-JS-L), Version 12.0(8), RELEASE SOFTWARE (fc1)
```

(Se cortó el desplegado)

```
Configuration register is 0x2142
```

y después de modificarlo con el comando **config-register**, el mismo comando **show version** muestra el valor del registro al proximo arranque:

```
Router(config)#config-register 0x2142
Router(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console
Router#show ver
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-JS-L), Version 12.0(8), RELEASE SOFTWARE (fc1)
```

(Se cortó el desplegado)

```
Configuration register is 0x2102 (will be 0x2142 at next reload)
```

El manejo del registro en el ruteador es en hexadecimal y la manera de decirle a un ruteador que el número escrito es hexadecimal es anteponiendo **0x** de modo que el cambiar el registro de 0x2102 a 0x2142 significa simplemente que se prendió el *bit* # 6. por supuesto que este cambio tendrá efecto hasta la próxima vez que arranque el ruteador.

6.3 Recuperación de Acceso a un Ruteador

Más veces de lo deseado, se presenta la situación en la que, legalmente, se necesita entrar a un ruteador pero no se cuenta con la palabra clave para hacerlo. Haciendo uso del registro de configuración es posible lograrlo.

El registro de configuración tiene un *bit* que le indica al ruteador ignorar el contenido de la NVRAM. Entre otras cosas, el contenido de la NVRAM es la configuración con la que se inicializa el ruteador (*startup-config*) y como se vio en el capítulo 4 en el tema "Configuración Guiada", cuando el ruteador no inicializa una configuración válida, entra en el modo de configuración guiada sin cargar la startup-config a la running-config. Ésta última característica es la que se aprovecha para ingresar a un ruteador sin conocer la clave de acceso.

```
Router Con0 is now available

Press RETURN to get started!

User Access Verification

Password:
Password:
Password:
Password:
```

Así comienza el proceso: dándose cuenta que no se tiene la clave de acceso. Si por cualquiera de las líneas de acceso se puede entrar al ruteador y luego al modo privilegiado no hay problema, pues desde modo privilegiado se pueden ver las claves o en última instancia sobrescribir nuevas. Supóngase que no hay otra línea de acceso disponible o que la clave de acceso que no se tiene es precisamente la necesaria para entrar al modo privilegiado.

El primer paso es prender el ruteador e interrumpir la secuencia de arranque. Para hacerlo se utiliza la combinación **Ctrl.+Break**

En ruteadores de la serie 2500:

```
System Bootstrap, Version 11.0(10c)XB1, PLATFORM SPECIFIC RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1997 by cisco Systems
2500 processor with 4096 Kbytes of main memory
Abort at 0x51C3 (PC)
>
```

En ruteadores de la serie 2600:

```
System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
Copyright (c) 1999 by cisco Systems, Inc.
TAC:Home:SW:IOS:Specials for Info
PC = 0xfff0a530, Vector = 0x500, SP = 0x680127b0
C2600 platform with 32768 Kbytes of main memory
PC = 0xfff0a530, Vector = 0x500, SP = 0x80004374
monitor: command "boot" aborted due to user interrupt
rommon 1 >
```

Recuérdese que no se ha cargado el IOS así que los comandos del IOS no se reconocen en este indicador.

Para modificar el registro se utiliza el comando **o/r** en la serie 2500 y **confreg** en la serie 2600. Para que el ruteador ignore la NVRAM, el *bit* # 6 en el registro de configuración se debe de encender. Lo que hace que el número en hexadecimal que tiene el registro desde fábrica se debe cambiar de 2102 a 2142.

Para ruteadores de la serie 2500:

```
>o/r 0x2142
```

Y para ruteadores de la serie 2600:

```
rommon 1 >confreg 0x2142
```

Después de ingresar este comando, la próxima vez que el ruteador inicie lo hará ignorando la NVRAM y no copiará el startup-config al running-config. Valiéndose de eso, se debe entrar al modo privilegiado y ya desde adentro copiar manualmente la configuración de NVRAM a RAM. Es muy importante no comenzar a trabajar antes de hacer esta copia y no guardar la RAM en NVRAM (*copy run start*) pues esto provocaría la sobreescritura de una configuración vacía, que es con la que se entró al ruteador sobre la configuración con la que el ruteador estaba funcionando.

Para reiniciar el ruteador se utiliza el comando **i** para la serie 2500 o **reset** para la serie 2600.

Para la serie 2500:

```
>i
```

para la serie 2600:

```
rommon 1 > reset
```

El comando anterior reinicia el ruteador y al arrancar éste, entrará en modo de configuración asistida. Es necesario recalcar la importancia de no entrar al diálogo de configuración puesto que sí se cuenta con una configuración de inicio; solamente que no se ha cargado.

```
Router Con0 is now available

Press RETURN to get started!

Would you like to enter the initial configuration dialog? [yes/no]:n
Router>
```

Dado que se está entrando a una configuración vacía, no hay palabras claves de acceso establecidas y de inmediato se puede entrar a modo usuario. Por la misma razón, nada impide que se entre a modo privilegiado. Ya en modo privilegiado se puede copiar manualmente la configuración de inicio a la configuración de trabajo (*copy startup-config running-config.*)

```
Router>enable
Router#copy start run
%SYS-5-CONFIG_I: Configured from memory by console
Router#show run
```

(Se seleccionaron algunas líneas de la respuesta del ruteador)

```
enable secret RnoLmJYuoLSo
enable password clave-habilitar
!
line con 0
 password clave-consola
```

Como se puede ver en la respuesta del ruteador, en este punto tan sólo es necesario pedir un desplegado de RAM para recuperar las claves que no están encriptadas. Las claves encriptadas no se pueden recuperar pero se pueden cambiar sin problema alguno pues ya se está en modo privilegiado.

El proceso no termina aquí, es muy importante volver a copiar la configuración ya modificada a la memoria NVRAM y regresar el valor del registro a 2102 para que la próxima vez que el ruteador arranque no ignore el contenido de NVRAM.

```
Router#copy run start
Destination filename [startup-config]? [ Enter ]
Warning: Attempting to overwrite an NVRAM configuration
previously written by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm] [ Enter ]
```

```
Building configuration...

[OK]
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#config-register 0x2102
Router(config)#exit
Router#
```

Se debe ser cuidadoso de cambiar la clave secreta, muchas veces se obtienen las demás claves y se olvida ésta. Lo que trae por resultado en la necesidad de realizar todo el proceso nuevamente por no poder ingresar al modo privilegiado.

6.4 Respaldo y Restauración de la Configuración

Una mágnifica práctica al resolver problemas relacionados con ruteadores, en especial si se acude en auxilio de empresas ajenas, es hacer un respaldo de la configuración actual y del IOS antes de comenzar a buscar el problema. Aún si se está seguro de que los cambios que se harán no tienen la menor influencia sobre el desempeño, funcionalidad, configuración o IOS del ruteador, conviene jugar a lo seguro. Por poco probable que sea, el peor de los casos es posible y es mejor estar prevenido para afrontarlo.

La forma más sencilla y práctica de respaldar tanto la configuración como el IOS de un ruteador es utilizando un servidor o una aplicación de TFTP.

Lo primero que se debe hacer es cerciorarse que el ruteador tiene conectividad al servidor TFTP. Este servidor puede ser remoto o estar en el mismo segmento que el ruteador, pero el ruteador debe tener conectividad al servidor. Personalmente, me gusta cargar una aplicación de servidor TFTP en mi computadora y al comenzar a trabajar en un ruteador conecto la tarjeta de red de mi computadora al mismo segmento en el que está el ruteador. Normalmente, habrá que pedir un IP al administrador local de la red ya que muchas redes cuentan con filtros de seguridad.

Una vez comprobada la conectividad del servidor hacia el TFTP se puede hacer un respaldo de la configuración de arranque, de la configuración corriente y del IOS. Para hacerlo se utiliza el comando **copy** desde modo privilegiado.

Recuérdese que el sistema operativo radica en flash. Para ver información acerca del o de los archivos que se encuentran en flash se utiliza el comando **show flash**

```
Router#show flash
System flash directory:
File  Length   Name/status
```

```
 1   8706380  /c3640-Is-mz_121-2.bIn
[8706444 bytes used,  8070772 avallable, 16777216 total]
16384K bytes of processor board System flash (Read ONLY)
```

Ahora se respalda el sistema operativo del ruteador:

```
Router#copy flash tftp
System flash directory:
File  Length   Name/status
 1  8706380  /c3640-Is-mz_121-2.bin
[8706444 bytes used, 8070772 avallable, 16777216 total]
Address or name of remote host [255.255.255.255]?172.16.0.2
```

El ruteador pide la dirección lógica del servidor TFTP o toma como valor predeterminado la dirección 255.255.255.255 que significa "todos los *hosts*" el término en inglés para esta dirección es *flooded broadcast* (la traducción literal del término da una idea del comportamiento de los paquetes que llevan esa dirección: Inundación de *broadcasts*.) El valor predeterminado significa que el ruteador buscará cualquier servidor TFTP para guardar en él el IOS.

```
Source file name? c3640-Is-mz_121-2.bIn
```

Nótese que el ruteador pide el nombre del archivo que se copiará, convenientemente este nombre aparece justo después de teclear el comando **copy flash** así que tan solo hay que copiarlo y pegarlo.

```
Destination file name [ c3640-Is-mz_121-2.bin ]? [Enter]
Verifying checksum for ' c3640-Is-mz_121-2.bIn '(file #1)...OK
Copy '/ c3640-is-mz_121-2.bin ' from Flash to server
as '/ c3640-is-mz_121-2.bIn '? [yes/no] y
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Upload to server done
Flash copy took 00:02:21 [hh:mm:ss]
Router#
```

Al igual que cuando se hace un Ping, el ruteador despliega un signo de admiración por cada segmento UDP que se recibe bien.

Para restaurar los archivos guardados en el TFTP al ruteador se utliza el mismo comando: **copy**, por supuesto que el orden de los parámetros se invierte.

Si al copiar un sistema operativo desde un TFTP hacia el ruteador hay memoria suficiente en flash para almacenar ambos sistemas operativos, el ruteador lo hace sin preguntar nada, pero si no lo hay, entonces da la opción de borrar el IOS actual para sobrescribir el nuevo archivo.

```
Router#copy tftp flash
                  **** NOTICE ****
Flash load helper v1.0
This process will accept the copy options and then terminate
the current system image to use the ROM based image for the copy.
Routing functionality will not be available during that time.
If you are logged in via telnet, this connection will terminate.
Users with console access can see the results of the copy operation.
                  --- ******** ----
Proceed? [confirm] [Enter]
System flash directory:
File  Length   Name/status
 1  8706380  /c3640-is-mz_121-2.bin
[8706444 bytes used, 8070772 available, 16777216 total]
Address or name of remote host[172.16.0.2]? [Enter]
```

Esta vez el ruteador, recuerda la dirección del servidor TFTP y la propone como predeterminada.

```
Source file name? c3640-is-mz_121-2.bin
Destination file name [ c3640-is-mz_121-2.bin ]?[Enter]
Accessing file 'dd' on 172.16.0.2...
Loading dd from 172.16.0.2 (via Ethernet0):[OK]
Erase flash device before writing?[confirm][Enter]
Flash contains files. Are you sure you want to erase?[confirm][Enter]
System configuration has been modified. Save?[yes/no]:y
Building configuration...

[OK]
Copy ' c3640-is-mz_121-2.bin ' from server
as ' c3640-is-mz_121-2.bin ' into Flash WITH erase?[yes/no]y
```

El ruteador pide varias veces la confirmación del proceso porque cambiar el IOS es una tarea delicada. Después de aceptar el proceso, el ruteador se reinicia y carga un sistema operativo mínimo para borrar el IOS actual y para cargar el nuevo IOS.

```
%SYS-5-RELOAD: Reload requested
%FLH: c3640-is-mz_121-2.bin from 172.16.0.2 to flash
...
 System flash directory:
File  Length   Name/status
  1   8706380  /c3640-is-mz_121-2.bin
[8706444 bytes used, 8070772 available, 16777216 total]
Accesing file ' c3640-is-mz_121-2.bin ' on 172.16.0.2
...
Loading  c3640-is-mz_121-2.bin .from 172.16.0.2
 (via Ethernet 0): ! [OK]

Erasing device ... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
 eeeeeeeeeeeeeeeeeeeeeeeeeee
```

Las letras "e" se despliegan para mostrar que se está borrando la memoria flash.

```
 Loading  c3640-is-mz_121-2.bin from 172.16.0.2
  (via Ethernet 0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

[OK - 8706380/16777216 bytes]

Verifying checksum... OK (0x18F5)
Flash copy took 0:05:16 [hh:mm:ss]
%FLH: Re-booting system after download
```

Después de que se ha copiado el nuevo IOS el ruteador se reinicia para utilizarlo.

El comando para copiar la configuración de arranque es: **copy startup-config tftp** y el comando para copiar la configuración corriente al servidor es: **copy running-config tftp**. Recuérdese que la configuración de arranque (*startup-config*) radica en NVRAM y la corriente (*running-config*) en RAM. También es posible copiar la configuración corriente a la de arranque para guardar los cambios realizados al ruteador con **copy run start**. El comando copy se puede combinar de distintas maneras para respaldar y restaurar los tres diferentes tipos de memoria en el ruteador de manera análoga a como se mostró para hacerlo con la memoria flash.

Por ejemplo, para copiar la memoria RAM a un servidor TFTP, se hace de la siguiente forma:

```
Router#copy run tftp
Address or name of remote host [172.16.0.2]?[Enter]
Destination file name [Router-confg]?[Enter]
!!
487 bytes copies in 12.236 secs (40 bytes/sec)
Router#
```

Y, para copiar el respaldo de RAM desde el servidor TFTP a la configuración corriente del ruteador simplemente se teclea el mismo comando pero con los parámetros invertidos:

```
Router#copy tftp run
Address or name of remote host [172.16.0.2]?[Enter]
Source filename[]?router-confg
Destination filename [running-config]?[Enter]
Accessing tftp://172.16.0.2/router-confg...
Loading router-confg from 172.16.0.2 (via Ethernet0):
!!
[OK - 487/4096 bytes]
487 bytes copied in 5.400 secs (97 bytes/sec)
Router#
00:38:31: %SYS-5-CONFIG: Configured from tftp://172.16.0.2/router-confg
Router#
```

Un comando útil al manejar la NVRAM es el comando **erase startup-config**. Este comando indica al ruteador borrar el contenido de la NVRAM y la siguiente vez que se reinicie el ruteador, éste entrará en modo de configuración asistida.[1]

```
Router#erase start
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
```

6.5 *Ping y Traceroute*

Ping y Traceroute son comandos del protocolo ICMP, que controla la conectividad en el stack TCP/IP. ICMP radica en la capa de red del modelo OSI, de modo que los comandos Ping y Traceroute permiten probar la conectividad hasta la capa de red entre dispositivos remotos.

[1] Véase la sección 4.1 "Modo de Configuración Guiada"

Sin duda alguna, la herramienta más utilizada para probar la conectividad en las redes es el comando Ping[2]. Este comando hace que el sistema desde que se emite mande un mensaje hacia un *host* remoto, solamente para confirmar que dicho mensaje puede llegar a él. El mensaje que se envía se llama *echo request* y el mensaje que el *host* remoto regresa para confirmar el arribo se llama *echo reply*. El comando ping se puede utilizar desde el modo usuario, así como desde el modo privilegiado, con una diferencia: desde el modo privilegiado se tiene la opción de utilizar la versión extendida del comando.

Por ejemplo, para probar si se tiene conectividad con el sitio www.celticrover.com[3] tan solo se tiene que utilizar el comando ping seguido del IP del sitio. Es más, también se puede dar el comando ping seguido del nombre del sitio siempre y cuando se cuente con un servicio de resolución de nombres como DNS (*Domain Name Service*) que devuelve el IP correspondiente al nombre de dominio que se le da. Normalmente, si se navega por Internet ya se cuenta con estos servicios, pero en una red privada hay que configurarlos. Por supuesto que es más fácil recordar celticrover.com que 216.119.75.101.

```
Router#ping www.celticrover.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 216.119.75.101, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/74/76 ms
Router#
```

La respuesta del ruteador muestra con signos de admiración que cada uno de los 5 ecos de 100*bytes* que envió ICMP fue recibido satisfactoriamente. El tiempo máximo que el ruteador espera para considerar que un eco se perdió es de dos segundos y el ruteador muestra que el viaje redondo *echo request-echo reply* fue de 72 milisegundos el menor, de 76 milisegundos el mayor y en promedio de 74. El contenido de los paquetes es simplemente el abecedario.

El ping extendido permite modificar muchos de los parámetros para el envío del eco. Al teclear desde modo privilegiado únicamente la palabra ping y pulsar [Enter], el ruteador inicia un pequeño asistente para configurar el ping extendido.

```
Router#ping
```

Al poner solamente la palabra ping, se inicia el asistente para configurar los parámetros del eco. Como en el caso del asistente para la configuración guiada, los valores predeterminados aparecen entre corchetes y para seleccionarlos se presiona la tecla [Enter].

---

[2] En las páginas 77 y 78 se discuten algunas características de Ping y Traceroute.
[3] En este sitio se ofrecen exámenes de preparación para presentar el examen CCNA de Cisco.

```
Protocol [ip]:[Enter]
Target IP address: www.celticrover.com
```

Al igual que con el ping normal, en este campo se puede poner el IP de destino o, si se utiliza una herramienta para la resolución de nombres, se puede utilizar un nombre.

```
Repeat count [5]: 1
Datagram size [100]:[Enter]
Timeout in seconds [2]: 1
```

El número de datagramas a enviar, el tamaño que éstos deben tener y el tiempo que el sistema debe esperar sin recibir respuesta, antes de considerar perdido un datagrama. A continuación se configuran los comandos extendidos. En el ejemplo se hará un barrido, variando el tamaño de los datagramas para determinar el tamaño del MTU que se ha negociado entre las tarjetas de red del emisor y el receptor.

```
Extended commands [n]: y
```

En el ejemplo se pide entrar a los comandos extendidos del ping extendido, (aún si no se entra en este menú extendido, se está utilizando un ping extendido.)

```
Source address: ethernet 0
Type of service [0]:[Enter]
```

El tipo de servicio puede ser 0 o 1 y determina la calidad del servicio de Internet, aún al especificarlo, este parámetro no necesariamente será considerado por todos los ruteadores en el recorrido del datagrama.

```
Set DF bit in IP header? [no]: y
```

El DF (*Don't Fragment*) es una bandera que indica al ruteador no dividir los datagramas a enviar. Normalmente, cuando un datagrama es mayor al tamaño de alguno de los buffers en la transmisión, éste no puede ser enviado en una sola carga, por lo tanto el datagrama se envía en dos o más fragmentos. En el ejemplo, al poner este *bit* en 1, se le pide al ruteador que no fragmente los datagramas, cuando el primer datagrama enviado no quepa en el buffer se producirá un error y así se conocerá el tamaño exacto del MTU.

```
Validate reply data? [no]: y
Data pattern [0xABCD]: 0xb38f
```

El ping extendido permite incluso especificar el patrón de *bit*s que se envía en el eco. En el ejemplo se desea enviar la siguiente secuencia: 10-1100-111000-1111. Para hacerlo, simplemente se le indica al ruteador el número en hexadecimal que se desea

enviar. (Recuérdese que el 0x significa que el número que le sigue está representado en hexadecimal.)

```
Loose, Strict, Record, Timestamp, Verbose[none]: v
Loose, Strict, Record, Timestamp, Verbose[V]:[Enter]
```

Loose permite especificar hops por los que se prefiere que el datagrama transite. Strict permite especificar hops por los que el datagrama debe transitar forzosamente. Timestamp sirve para conocer el tiempo del viaje redondo a un *host* en particular. La opción verbose pide desplegar en pantalla la información conforme se va obteniendo. Esta opción se selecciona automáticamente al seleccionar cualquier otra. Record es una opción muy útil que permite conocer hasta nueve hops en el trayecto que sigue el eco incluyendo los que hace el *echo request* hacia el *host* remoto y los que hace el *echo replay* de regreso hacia el *host* que envió el ping.

```
Sweep range of sizes [n]: y
Sweep min size [32]: 1400
Sweep max size [18024]: 1520
Sweep interval [1]: 5
```

Se hará un barrido de tamaños de datagramas, comenzando desde un datagrama de 1400 *bytes* hasta uno de 1520 incrementado sus tamaños de 5 en 5 *bytes*. Al ingresar el último valor requerido, el ruteador comienza a enviar la sucesión de ecos con la secuencia y demás parámetros especificados:

```
Type escape sequence to abort.
Sending 25, [1400..1520]-byte ICMP Echos to 216.119.75.101, timeout is 1 seconds
:
Packet has data pattern 0xB38F
Reply to request 0 (148 ms) (size 1400)
Reply to request 1 (152 ms) (size 1405)
Reply to request 2 (148 ms) (size 1410)
Reply to request 3 (148 ms) (size 1415)
Reply to request 4 (148 ms) (size 1420)
Reply to request 5 (148 ms) (size 1425)
Reply to request 6 (148 ms) (size 1430)
Reply to request 7 (148 ms) (size 1435)
Reply to request 8 (148 ms) (size 1440)
Reply to request 9 (148 ms) (size 1445)
Reply to request 10 (152 ms) (size 1450)
Reply to request 11 (152 ms) (size 1455)
Reply to request 12 (152 ms) (size 1460)
Reply to request 13 (152 ms) (size 1465)
Reply to request 14 (156 ms) (size 1470)
```

```
Reply to request 15 (152 ms) (size 1475)
Reply to request 16 (148 ms) (size 1480)
Reply to request 17 (152 ms) (size 1485)
Reply to request 18 (152 ms) (size 1490)
Unreachable from 172.16.0.1, maximum MTU 1492 (size 1495)
Unreachable from 172.16.0.1, maximum MTU 1492 (size 1500)
Request 21 timed out (size 1505)
Request 22 timed out (size 1510)
Request 23 timed out (size 1515)
Request 24 timed out (size 1520)
Success rate is 76 percent (19/25), round-trip min/avg/max = 148/150/156 ms
Router#
```

Dado que no se permitió la fragmentación de los datagramas se pudo conocer el MTU (1492) y el tiempo que toma el viaje redondo hasta este sitio (150ms aproximadamente) en la transmisión a celticrover.com.

Traceroute es en realidad una versión de ping. Traceroute es la versión para ruteadores del comando tracert. Traceroute permite conocer la ruta que sigue un datagrama para alcanzar un *host* remoto. Para hacer esto, el emisor genera varios datagramas con tiempos de vida que se van incrementando (aunque el término TTL, *Time To Live*, se refiere a tiempo, la unidad que utiliza es hops) comenzando con un hop y llegando hasta 30 hops de manera predeterminada. Estos paquetes se envían con destino a un puerto inválido que por *default* es 33434. al enviar el primer paquete, el tiempo de vida de éste se fija en 1 hop pero recuérdese que cada ruteador que recibe un paquete decrementa el TTL en éste. Entonces el primer ruteador que recibe el primer datagrama UDP enviado hace que el TTL se convierta en cero, cuando el TTL de un paquete llega a cero, el ruteador que lo recibe lo elimina y envía un mensaje de "Tiempo de vida excedido" hacia el emisor. El emisor recibe el paquete de tiempo de vida excedido y registra los datos del ruteador que envió esta respuesta. Entonces, el emisor manda un paquete similar al anterior pero con TTL de 2 saltos. Este datagrama llega al segundo ruteador en donde es eliminado y se genera una respuesta con los datos del ruteador que el emisor original registra. Y así sucesivamente hasta que el paquete llega a su destino o se alcanza el valor máximo del TTL del Traceroute (30 por *default.*) Si el datagrama llega a su destino, el *host* de destino responde con un mensaje de "Puerto inalcanzable" ya que el puerto es inválido. Cuando el emisor que generó el paquete recibe este mensaje almacena los datos del dispositivo que respondió y termina el proceso de Traceroute.

El comando Traceroute se puede ejecutar desde modo usuario y desde modo privilegiado.

Al hacer un Traceroute hacia celticrover.com se obtiene la siguiente respuesta:

```
Router#traceroute www.celticrover.com
```

```
Translating "www.celticrover.com"...domain server (255.255.255.255) [OK]

Type escape sequence to abort.
Tracing the route to www.celticrover.com (216.119.75.101)

 1 172.16.0.1 4 msec 4 msec 4 msec
 2 inet-pue-lapaz-1-l0.uninet-ide.com.mx (148.223.240.77) 12 msec 12 msec 12 msec
 3 inet-pue-fuertes-1-pos4-1.uninet.net.mx (148.223.240.70) 12 msec 16 msec 12 msec
 4 bup-pue-fuertes-1-g8-0.uninet.net.mx (200.38.203.34) 12 msec 12 msec 12 msec
 5 bup-pue-ctp-9-pos7-0.uninet.net.mx (200.38.193.98) 16 msec 16 msec 16 msec
 6 bb-pue-ctp-8-g9-0.uninet.net.mx (200.38.202.49) 16 msec 16 msec 16 msec
 7 bb-mex-nextengo-11-pos7-0.uninet.net.mx (200.38.193.58) 16 msec 20 msec 16 msec
 8 inet-cal-onewilshire-1-pos7-0.uninet.net.mx (200.38.209.10) 60 msec 56 msec 56 msec
 9 lsanca1wcx1-gige13-0.wcg.net (64.200.139.133) 72 msec 68 msec 72 msec
10 anhmca1wcx2-pos4-0.wcg.net (64.200.240.209) 72 msec 72 msec 72 msec
11 phnxaz1wce2-pos4-0.wcg.net (64.200.240.22) 80 msec 76 msec 80 msec
12 phnxaz1wce2-sterlingnet-gige.wcg.net (65.77.92.70) 76 msec 80 msec 80 msec
13 ip-206-83-192-6.sterlingnetwork.net (206.83.192.6) 72 msec 72 msec 72 msec
14 216.119.107.1 72 msec 72 msec 72 msec
15 216.119.107.9 72 msec 68 msec 72 msec
16 www.celticrover.com (216.119.75.101) 72 msec 72 msec 68 msec
Router#
```

Al igual que el comando ping, el comando Traceroute cuenta con una versión extendida, y ésta también se accesa solamente desde el modo privilegiado de ejecución en el ruteador.

```
Router#traceroute
Protocol [ip]:[Enter]
Target IP address: www.celticrover.com
Source address: 172.16.224.255
Numeric display [n]:[Enter]
Timeout in seconds [3]: 1
Probe count [3]: 1
Minimum Time to Live [1]:[Enter]
Maximum Time to Live [30]:[Enter]
Port Number [33434]:[Enter]
Loose, Strict, Record, Timestamp, Verbose[none]:[Enter]
Type escape sequence to abort.
Tracing the route to www.celticrover.com (216.119.75.101)

 1 172.16.0.1 4 msec
 2 inet-pue-lapaz-1-l0.uninet-ide.com.mx (148.223.240.77) 12 msec
```

```
 3 inet-pue-fuertes-1-pos4-1.uninet.net.mx (148.223.240.70) 16 msec
 4 bup-pue-fuertes-1-g8-0.uninet.net.mx (200.38.203.34) 12 msec
 5 bup-pue-ctp-9-pos7-0.uninet.net.mx (200.38.193.98) 16 msec
 6 bb-pue-ctp-8-g9-0.uninet.net.mx (200.38.202.49) 16 msec
 7 bb-mex-nextengo-11-pos7-0.uninet.net.mx (200.38.193.58) 20 msec
 8 inet-cal-onewilshire-1-pos7-0.uninet.net.mx (200.38.209.10) 56 msec
 9 lsanca1wcx1-gige13-0.wcg.net (64.200.139.133) 72 msec
10 anhmca1wcx2-pos4-0.wcg.net (64.200.240.209) 72 msec
11 phnxaz1wce2-pos4-0.wcg.net (64.200.240.22) 76 msec
12 phnxaz1wce2-sterlingnet-gige.wcg.net (65.77.92.70) 80 msec
13 ip-206-83-192-6.sterlingnetwork.net (206.83.192.6) 68 msec
14 216.119.107.1 68 msec
15 216.119.107.9 68 msec
16 www.celticrover.com (216.119.75.101) 72 msec
Router#
```

Tanto en el ping extendido como en el Traceroute extendido si se quiere abortar una secuencia de datagramas que se están enviando, se teclea la combinación **Ctrl.+Shift+6**.

Si se conocen los parámetros que se pueden modificar tanto en el ping extendido como en el Traceroute extendido, se podrán aprovechar al máximo estas herramientas tan poderosas del protocolo ICMP.

6.6 Telnet

Telnet[4] es un método de conexión que radica en la capa de aplicación del modelo DoD. La mejor forma de comprobar conectividad entre las capas de aplicación de dos sistemas que utilizan TCP/IP es Telnet.

Telnet emula la línea de comando de un *host* remoto a través de la red. Para poder hacer uso de Telnet hacia un ruteador, es necesario que éste tenga configurada una palabra clave de acceso para Telnet (*line vty.*)

De manera predeterminad

```
Router-local#172.16.224.255
Trying 172.16.224.255 ... Open

User Access Verification

password:
Router-remoto>
```

Para salir de la sesión se utiliza el comando **exit**

```
Router-remoto>exit
[Connection to 172.16.224.255 closed by foreign host]

Router-local#
```

En caso de desear regresar a la línea de comando del ruteador local sin cerrar la sesión de Telnet en el ruteador remoto, se utiliza la secuencia **Ctrl.+Shift+6 , X** (se presionan las tres primeras teclas simultáneamente, se sueltan y de inmediato se presiona la "x".)

```
Router-remoto> [Ctrl.+Shift+6 y despues X]
Router-local#
```

Al teclear la combinación dada, se regresa a la línea de comando del ruteador local pero no se cerró la conexión por Telnet al *host* remoto, el comando **show sessions** muestra las sesiones Telnet que un ruteador local tiene esta

Ahora hay dos sesiones abiertas y al pedir un desplegado de las sesiones se muestran ambas y frente a la última utilizada se muestra un asterisco. Para regresar a la última sesión que se utilizó tan solo se presiona dos veces la tecla [Enter].

```
Otro-remoto>[Ctrl.+Shift+6 y despues X]
Router-local#show sessions
Conn Host          Address          Byte  Idle Conn Name
  1  172.16.224.255  172.16.224.255  0     1    172.16.224.255
* 2  172.16.40.2     172.16.40.2     0     1    172.16.40.2
Router-local#[Enter][Enter]
[Resuming connection 2 to 172.16.40.2 ... ]

Otro-remoto>
```

También se puede accesar a otras sesiones simplemente poniendo el número de la conexión y presionando dos veces [Enter]. Para cerrar una sesión abierta a un *host* remoto pero desde la línea de comando del ruteador local se utiliza el comando **disconnect** seguido de la conexión que se desea cerrar.

```
Otro-remoto>[Ctrl.+Shift+6 y despues X]
Router-local#show sessions
Conn Host          Address          Byte  Idle Conn Name
  1  172.16.224.255  172.16.224.255  0     1    172.16.224.255
* 2  172.16.40.2     172.16.40.2     0     1    172.16.40.2
Router-local# disconnect 2
Closing connection to 172.16.40.2 [confirm] [Enter]
Router-local#
```

Por otro lado es posible monitorear las sesiones remotas abiertas desde otros dispositivos hacia un ruteador local con el comando **show users** y para cerrar la sesión que un usuario remoto tiene abierta en un ruteador local se utiliza el comando clear line seguido del número de usuario que se quiere desconectar.

```
Router-local#show users
  Line    User     Host(s)          Idle Location
* 0 con 0          idle             9
  1 aux 0          Idle             0
  2 vty 0          idle             0     172.16.12.5
Router-local#clear line 2
[confirm]
[OK]
```

En este caso, el asterisco indica cual de esas conexiones es la que está usando uno mismo.

Los nombres de los ruteadores tienen alcance local, lo que significa que no es posible iniciar una sesión Telnet simplemente dando el nombre del ruteador al que se desea conectar:

```
Router-local#telnet Router-remoto
Translating 'Router-remoto'... domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
Router-local#
```

No es posible, a menos claro, que el nombre del ruteador que se busca pueda ser resuelto por un servidor DNS (tal como se mostró en la sección *"Ping y Traceroute"*) o resuelto por una tabla de correspondencia en el ruteador en el que se emite el Telnet. Para añadir entradas a la tabla de correspondencia se utliza el comando **IP host** desde modo de configuración global.

```
Router-local(config)#ip host router-remoto 172.16.30.1
Router-local(config)#ip host otro-remoto 172.16.40.2
```

Y para ver dichas entradas se utiliza el comando **show hosts** desde modo privilegiado.

```
Router-local#show hosts
Default domain is not set
Name/address lookup uses domain service
Name servers are 255.255.255.255

Host                 Flags      Age Type   Address(es)
otro-remoto          (perm, OK) 0   IP     172.16.40.2
router-remoto        (perm, OK) 0   IP     172.16.30.1
```

Por supuesto que esta tabla también tiene sólo alcance local pero así ya se puede hacer Telnet (u otras funciones como *Ping y Traceroute*) por nombre.

```
Router-local#otro-remoto
Trying 172.16.40.2 ... Open

User Access Verification

Password:
Otro-remoto>
```

En el escenario 6.1 se utiliza la herramienta Telnet en conjunto con CDP.

6.7 CDP

CDP (*Cisco Discovery Protocol*) es un protocolo que permite obtener información de los dispositivos directamente conectados a un *switch* o ruteador local. CDP fue diseñado por Cisco y para equipos Cisco por lo que solamente funciona en este tipo de dispositivos.

CDP está habilitado de manera predefinida en los *switches* y ruteadores y sus comandos básicos son:

- **cdp run**. Desde modo de configuración global, este comando habilita la función de CDP a nivel global, CDP manda y recibe paquetes de información por todas las interfases activas del dispositivo. Para detener completamente el flujo de información CDP en todo el dispositivo se utiliza el comando **no cdp run**.

```
Router(config)#no cdp run
Router(config)#cdp run
```

- **cdp enable**. Este comando se utiliza desde modo de configuración de interfase y permite habilitar CDP exclusivamente en esa interfase. Para deshabilitar CDP de una interfase en particular se utiliza el comando **no cdp enable** desde el modo de configuración de la interfase.

```
Router(config-if)#no cdp enable
Router(config-if)#cdp enable
```

- **cdp timer**. Permite definir el periodo entre envío de paquetes CDP. Este comando se aplica desde modo de configuración global.

```
Router(config)#cdp timer 90
```

- **cdp holdtime**. Se utiliza para determinar el tiempo que se deben mantener los paquetes CDP recibidos de los dispositivos directamente conectados. Este comando, al igual que **cdp timer** se utiliza desde modo de configuración global.

```
Router(config)#cdp holdtime 240
```

- **show cdp**. Desde modo privilegiado, **show cdp** muestra la configuración global de cdp.

```
Router#show cdp
Global CDP information:
        Sending CDP packets every 90 seconds
        Sending a holdtime value of 240 seconds
```

- **show cdp neighbor**. Este comando y su variante **show cdp neighbor details** son la razón de existir de CDP, ya que muestran la información recabada del flujo de paquetes CDP acerca de los vecinos inmediatos al ruteador o *switch* en el cual se emita el comando.

```
Router#sh cdp nei
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID       Local Intrfce     Holdtme    Capability  Platform  Port ID
triangulo            Eth 0          240           S          1900      1
cuadrado             Ser 0          120           R          2621      Ser 0/1
circulo              Ser 1          120           R          2500      Ser 0
Router#
```

Nótese en la respuesta del ruteador: que el dispositivo tríangulo es un *switch*, el cual está conectado con el puerto 1 a la interfase *Ethernet* 0 del ruteador local, la plataforma del *switch* es un IOS 1900 y el tiempo que se mantendrá esa información si no hay otro paquete que la renueve es de 240 segundos. Véanse las características de los dispositivos cuadrado y círculo.

```
Router#sh cdp nei de
-------------------------
Device ID: triangulo
Entry address(es):
  IP address: 172.16.10.5
Platform: 1900,  Capabilities: Switch
Interface: Ethernet0,  Port ID (outgoing port): 1
Holdtime : 240 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C1900 Software (C1900-DOS-M), Version 12.0(4)T,  RELEASE SOFTWARE (fc1)

Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 23-Aug-03 00:32 by rpmg:

advertisement version: 1
-------------------------
Device ID:cuadrado
Entry address(es):
  IP address: 172.16.70.2
Platform: 2621,  Capabilities: Router
Interface: Serial0,  Port ID (outgoing port): Ser 0/1
```

```
Holdtime : 120 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-DOS-M), Version 12.0(4)T,  RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 23-Aug-03 00:32 by rpmg:
advertisement version: 1
---------------------

Device ID: circulo
Entry address(es):
  IP address: 172.16.90.1
Platform: 2500,  Capabilities: Router
Interface: Serial1,  Port ID (outgoing port): Ser 0
Holdtime : 120 sec
Version :
Cisco Internetwork Operating System Software
IOS (tm) C2500 Software (C2500-DOS-M), Version 12.0(4)T,  RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 23-Aug-03 00:32 by rpmg:

advertisement version: 1
Router#
```

Como se puede observar, **show cdp neighbor details** realmente da más detalles acerca de los vecinos al dispositivo desde donde se introduce el comando.

- **show cdp traffic**. Muestra estadísticas acerca de los paquetes cdp enviados y recibidos por un dispositivo.

```
Router#show cdp tra
CDP counters :
 Packets output: 26, Input: 19
 Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
  No memory: 0, Invalid packet: 0, Fragmented: 0
Router#
```

- **show cdp interface**. Muestra información acerca de las interfases que tienen habilitado CDP en el dispositivo local.

```
Router#show cdp int
Ethernet 0 is up, line protocol is up
```

Encapsulation ARPA
Sending CDP packets every 60 seconds
holdtime is 180 seconds

Escenario 6.1

Se desea descubrir la distribución de dispositivos Cisco en una red. Por motivos de logística, es imposible tener acceso físico a los dispositivos. Sin embargo, se sabe que CDP se ha dejado con los valores de fábrica y que la clave de acceso por Telnet es "Telnet" en todos ellos. La red cuenta con conectividad total y se tiene acceso a las computadoras. También se sabe que una de las interfases de alguno de los ruteadores tiene el IP 172.16.10.1.

A través del uso de CDP y de Telnet se puede definir la estructura de la red. Para comenzar se utiliza cualquier computadora para realizar una conexión por Telnet al IP conocido.

```
C:\>Telnet 172.16.10.1
 caballo>show cdp nei detail
 ------------------------
 Device ID: jaque
 Entry address(es):
   IP address: 172.16.10.5
 Platform: 1900,  Capabilities: Switch
 Interface: Ethernet0,  Port ID (outgoing port): 1
 Holdtime : 166 sec

 Version :
 Cisco Internetwork Operating System Software
 IOS (tm) C1900 Software (C1900-DOS-M), Version 12.0(4)T,  RELEASE SOFTWARE (fc1)

 Copyright (c) 1986-1999 by cisco Systems, Inc.
 Compiled Wed 19-Aug-99 17:29 by remg

 advertisement version: 1
 ------------------------
 Device ID: rey
 Entry address(es):
   IP address: 172.16.70.2
 Platform: 2621,  Capabilities: Router
 Interface: Serial0,  Port ID (outgoing port): Ser 0/1
 Holdtime : 120 sec

 Version :
```

Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-DOS-M), Version 12.0(4)T, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 28-Apr-99 17:29 by rmg
advertisement version: 1

Device ID: torre
Entry address(es):
IP address: 172.16.90.1
Platform: 2500, Capabilities: Router
Interface: Serial1, Port ID (outgoing port): Ser 0
Holdtime : 120 sec
Version :
Cisco Internetwork Operating System Software
IOS (tm) C2500 Software (C2500-DOS-M), Version 12.0(4)T, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 03-May-99 17:29 by rmga
advertisement version: 1

Con la información obtenida se puede saber lo mostrado en la figura 6.2

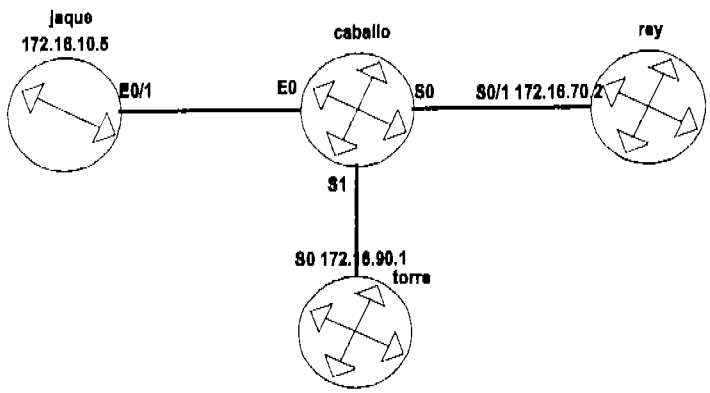


Figura 6.2 Parte descubierta de la red con un Telnet y CDP.

caballo>**telnet 172.16.10.5**
Trying 172.16.10.5 ...

Catalyst 1900 Management Console
Copyright (c) Cisco Systems, Inc. 1993-1999
All rights reserved.
Enterprise Edition Software
Ethernet Address: 00-30-80-C7-BE-C0

```
PCA Number:            73-3122-04
PCA Serial Number:     FAB033723WJ
Model Number:          WS-C1912-A
System Serial Number:  FAB0338S10A
Power Supply S/N:      APQ032404SA
PCB Serial Number:     FAB033723WJ,73-3122-04
-------------------------------------------

1 user(s) now active on Management Console.

      User Interface Menu

    [M] Menus
    [K] Command Line

Enter Selection:

      CLI session with the switch is open.
      To end the CLI session, enter [Exit].
jaque>show cdp nei
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, P - Repeater,    H - Host, I - IGMP
DeviceID    IP_Addr       Local_Port  Capability Platform      Remote_Port
caballo     172.16.10.1     Eth 0/1         R       2500          Eth 0
jaque>
```

CDP desde jaque muestra que este *switch* solo esta conectado a caballo y que el IP de la interfase E0 de caballo es 172.16.10.1

```
jaque>telnet 172.16.90.1
Trying 172.16.90.1 ... Open

User Access Verification

Password:

tone>show cdp nei detail
-------------------------
Device ID: caballo
Entry address(es):
  IP address: 172.16.90.2
Platform: 2500,  Capabilities: Router
Interface: Serial0,  Port ID (outgoing port): Ser 1
```

```
Holdtime : 120 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2500 Software (C2500-DOS-M), Version 12.0(4)T,  RELEASE SOFTWARE (fc1)

Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 03-May-99 17:29 by rmga

advertisement version: 1
-------------------------
Device ID: rey
Entry address(es):
  IP address: 172.16.80.1
Platform: 2621,  Capabilities: Router
Interface: Serial1,  Port ID (outgoing port): Ser 0/0
Holdtime :120 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-DOS-M), Version 12.0(4)T,  RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 28-Apr-99 17:29 by rmga
advertisement version: 1
torre>
```

Con la información que se tiene al momento, el diagrama crece así:

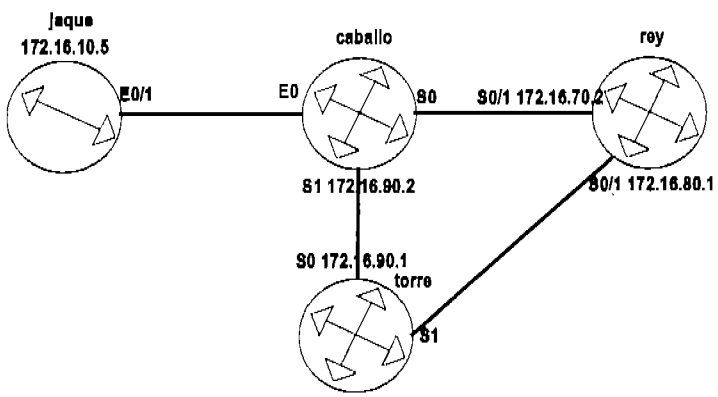


Figura 6.3 Diagrama estructural después de tres Telnet y CDP

```
torre>telnet 172.16.80.1
Trying 172.16.80.1 ... Open
```

User Access Verification

Password:
rey>**show cdp nei detail**

Device ID: gambito
Entry address(es):
IP address: 172.16.40.5
Platform: 1900, Capabilities: Switch
Interface: FastEthernet0/0, Port ID (outgoing port): 1
Holdtime : 120 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C1900 Software (C1900-DOS-M), Version 12.0(4)T, RELEASE SOFTWARE (fc1)

Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 19-Aug-99 17:29 by rmmg

advertisement version: 1

Device ID: enroque
Entry address(es):
IP address: 172.16.20.5
Platform: 1900, Capabilities: Switch
Interface: FastEthernet0/1, Port ID (outgoing port): 1
Holdtime : 120 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C1900 Software (C1900-DOS-M), Version 12.0(4)T, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 19-Aug-99 17:29 by armg
advertisement version: 1

Device ID: torre
Entry address(es):
IP address: 172.16.80.2
Platform: 2500, Capabilities: Router
Interface: Serial0/0, Port ID (outgoing port): Ser 1
Holdtime : 120 sec
Version :
Cisco Internetwork Operating System Software

```
IOS (tm) C2500 Software (C2500-DOS-M), Version 12.0(4)T,  RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 03-May-99 17:29 by rmgs:
advertisement version: 1
---------------------
Device ID: caballo
Entry address(es):
  IP address: 172.16.70.1
Platform: 2500,  Capabilities: Router
Interface: Serial0/1,  Port ID (outgoing port): Ser 0
Holdtime : 120 sec
Version :
Cisco Internetwork Operating System Software
IOS (tm) C2500 Software (C2500-DOS-M), Version 12.0(4)T,  RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 03-May-99 17:29 by ermg:
advertisement version: 1
rey>
```

Después de esta serie de comandos se descubrieron un par de *switches* más en la red: enroque con una IP de 172.16.20.5 y gambito cuya IP es 172.16.40.5

```
rey>172.16.40.5
Trying 172.16.40.5 ...

Catalyst 1900 Management Console
Copyright (c) Cisco Systems, Inc.  1993-1999
All rights reserved.
Enterprise Edition Software
Ethernet Address:     00-30-80-C7-BE-C0

PCA Number:           73-3122-04
PCA Serial Number:    FAB033723WJ
Model Number:         WS-C1912-A
System Serial Number: FAB0338S10A
Power Supply S/N:     APQ032404SA
PCB Serial Number:    FAB033723WJ,73-3122-04
-------------------------------------------

1 user(s) now active on Management Console.

      User Interface Menu
```

```
    [M] Menus
    [K] Command Line

Enter Selection:

    CLI session with the switch is open.
    To end the CLI session, enter [Exit].
gambito>show cdp nei
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, P - Repeater,    H - Host, I - IGMP
DeviceID    IP_Addr      Local_Port  Capability Platform     Remote_Port
dama        172.16.40.2  Eth 0/7     R          2500         Eth 0
rey         172.16.40.1  Fas 0/26    R          2621         Fas 0/0
gambito>
```

Un descubrimiento más: el ruteador dama cuya E0 es 172.16.40.2.

```
gambito>172.16.40.2
Trying 172.16.40.2 ... Open

User Access Verification

Password:
dama>show cdp nei det
----------------------
Device ID: gambito
Entry address(es):
  IP address: 172.16.40.5
Platform: 1900,  Capabilities: Switch
Interface: Ethernet0,  Port ID (outgoing port): 1
Holdtime : 120 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C1900 Software (C1900-DOS-M), Version 12.0(4)T,  RELEASE SOFTWARE (fc1)

Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 19-Aug-99 17:29 by mmfg

advertisement version: 1
dama>
```

Nada nuevo. Dama es el último rutcador en esta línea. Cambiando de rumbo, se ven las conexiones directas a enroque.

```
dama>172.16.20.5
Trying 172.16.20.5 ...

Catalyst 1900 Management Console
Copyright (c) Cisco Systems, Inc.  1993-1999
All rights reserved.
Enterprise Edition Software
Ethernet Address:    00-30-80-C7-BE-C0

PCA Number:          73-3122-04
PCA Serial Number:   FAB033723WJ
Model Number:        WS-C1912-A
System Serial Number: FAB0338S10A
Power Supply S/N:    APQ032404SA
PCB Serial Number:   FAB033723WJ,73-3122-04
-------------------------------------------

1 user(s) now active on Management Console.

     User Interface Menu

   [M] Menus
   [K] Command Line

Enter Selection:

    CLI session with the switch is open.
    To end the CLI session, enter [Exit].
enroque>show cdp nei
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, P - Repeater,    H - Host, I - IGMP
DeviceID    IP_Addr       Local_Port  Capability Platform      Remote_Port
rey         172.16.20.1     Fas 0/26        R       2621        Fas 0/1
enroque>
```

Enroque es el último dispositivo en esta línea. Por lo tanto el diagrama completo investigado se muestra en la figura 6.4:

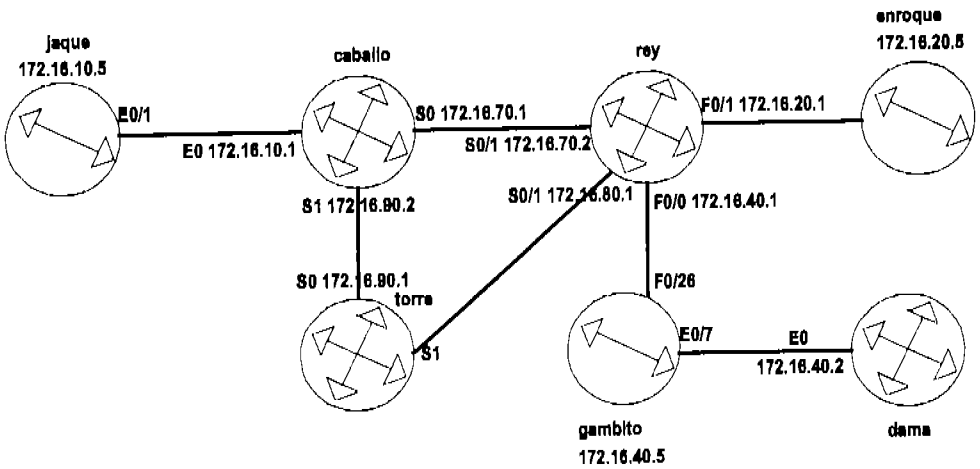


Figura 6.4 Diagrama de la red completa.

Conclusiones

Este manual es una compilación y depuración del material que he utilizado desde hace más de tres años en la preparación de profesionales certificados. Lo que en un principio eran cientos de lecturas y varios manuales de referencia (casi en su totalidad escritos en ingles), evolucionó hasta llegar a ser la serie de conceptos que se presentan, y están orientados al aprendizaje progresivo y por consecuencia a la aprobación del examen de Cisco.

Existen múltiples manuales y bibliografía en español sobre el tema de las redes de computadoras. Sin embargo, ninguno de ellos esta orientado a los conceptos prácticos que las industrias realmente necesitan y ponen por manifiesto en los objetivos de los exámenes de certificación internacional. El presente trabajo, lejos de ser una mera traducción de varias fuentes en ingles, es un manual pensado y diseñado para profesionales del área de la computación de habla hispana. Y aunque, presumiblemente puede ser utilizado con los mismos resultados por personas hispano parlantes de varias nacionalidades, fue específicamente pensado para profesionales mexicanos.

El manual que se presenta en este trabajo es una sucesión de temas que siguen un orden lógico y progresivo el cual fue determinado por experiencia propia al prepararme para aprobar, yo mismo, este examen, y más adelante al ayudar a otros profesionales a conseguir el mismo logro. La secuenciación de los temas a la que llegué ha sido ya utilizada por algún tiempo por todos los instructores en el centro de certificaciones en el que laboro para facilitar a sus grupos la consecución de una o más certificaciones en el área de las redes.

Muchos de los temas que se tratan en este manual, normalmente no son materia de mucho estudio en otros manuales, por lo que para dominar esos temas era necesario recurrir a varias fuentes de información. Este manual trata esos temas de manera concisa, pero a la vez cuidando los detalles que la industria requiere y que Cisco valora en sus exámenes de certificación. Por otro lado, la información que se da en cada tema no es extensa si ésta no representa uno de los dominios cotizados por Cisco. En más de un tema, se ha buscado quitar el sentido estrictamente técnico para facilitar la comprensión del concepto central que se necesita dominar para utilizar la herramienta en el campo laboral. Además, se incluyeron en el temario de este manual algunos temas que actualmente no son parte del temario del examen pero que a mi criterio personal son fundamentales para el manejo integral de las redes. Asimismo, se incluyen temas que en un futuro podrían formar parte de los requerimientos de Cisco.

A la fecha de la conclusión de este manual (Noviembre de 2004), el temario cubre todos los temas que Cisco publica como fundamentales para lograr la certificación. Sin embargo, como parte de la actualización del proyecto, se publicarán artículos relacionados con los nuevos objetivos que Cisco requiera y que no estén incluidos en

el manual. Estos artículos se publicarán en la siguiente dirección: www.raul.enpuebla.com.mx.

Actualmente, unas 50 personas han conseguido certificarse utilizando alguna versión del material que, después de destilarse ha llegado a ser este manual. Sin embargo, siendo completamente objetivo al respecto, esto no es realmente un indicador absoluto de que el material funcione al utilizarse de manera exclusiva en la preparación del examen, ya que la mayor parte de las personas que lo han utilizado, también han contado con mi ayuda como instructor. De hecho, el objetivo de este manual no es que se le use de manera exclusiva para la preparación del examen sino como base de un estudio más completo.

Varias de las personas certificadas han conseguido mejores trabajos o aumentos o logrado ascensos gracias a su certificación. Algunas de ellas han tenido la oportunidad de cambiar su lugar de residencia a la Ciudad de México, a Canadá, a Estados Unidos y a Inglaterra.

No cabe duda que el objetivo principal de este manual se cumple al proveer una herramienta importante para que las personas interesadas en obtener una certificación internacional en el campo de las redes computacionales lo puedan hacer de una manera eficaz, flexible y económica. Pero, ¿Qué tan importante es esta herramienta? –creo que ahora que el trabajo en la creación del manual ha terminado, comienza el trabajo para que este material realmente represente un beneficio para muchas personas. Si bien, no fue un objetivo particular de este trabajo como tesis, un objetivo personal es que este material facilite un cambio positivo y notable en la posición internacional que tiene México en cuanto a las tecnologías de la información. En este sentido, la conclusión de la tesis es que el objetivo de dar una alternativa flexible y económica para lograr obtener una de las certificaciones internacionales más buscadas por la industria se cumplió cabalmente, pero además de una conclusión es la constancia de un reto personal por mejorar México. El siguiente paso en este reto, también ya se esta dando, ya que el material, resultado de este trabajo será el libro de texto, a partir del próximo ciclo, en los cursos de redes en la Universidad especializada en las Tecnologías de la Información en donde laboro.

Este manual puede, sin duda, ayudar a satisfacer la expectación de ser seres humanos realizados dentro del contexto de sus trabajos a muchas personas, ya que permite alcanzar metas parciales hacia esa realización, como son:

- Conocer los aspectos fundamentales en la teoría de redes y en el manejo de sistemas Cisco para ofrecer un trabajo más eficiente.

- Tener una visión amplia en el manejo de las redes que permita optimizar los recursos de una manera sustentable en sus empresas.

- Lograr una certificación internacional otorgada por una de las industrias más reconocidas a nivel mundial. (con este manual es posible prepararse para aprobar el examen 640-821 INTRO de Cisco y también cubre los objetivos del examen N10 Network + experto en redes de CompTIA)

Creo realmente, que esta herramienta puede ayudar a muchas personas a "Ser todo lo que pueden ser" tal como se planteo en el objetivo del trabajo.

Apéndices

Apéndice A

Listado de todas las sub-redes posibles en un octeto IP

En este apéndice se muestran todos los identificadores de red que puede tener un solo octeto IP al utilizar máscaras de sub-red variables. Al inicio de cada columna se muestra la máscara del octeto. Se debe recordar que aunque es muy útil conocer los identificadores en un octeto del IP, siempre se debe considerar la totalidad del IP al analizar y planear la asignación de IP's en una red.

128	192	224	240	248	252	254	255
0	0	0	0	0	0	0	0
							1
						2	2
							3
					4	4	4
							5
						6	6
							7
				8	8	8	8
							9
						10	10
							11
					12	12	12
							13
						14	14
							15
			16	16	16	16	16
							17
						18	18
							19
					20	20	20
							21
						22	22
							23
				24	24	24	24
							25
						26	26
							27
					28	28	28
							29
						30	30
							31
		32	32	32	32	32	32
							33
						34	34
							35
					36	36	36
							37

					38	38
						39
			40	40	40	40
						41
					42	42
						43
				44	44	44
						45
					46	46
						47
		48	48	48	48	48
						49
					50	50
						51
				52	52	52
						53
					54	54
						55
			56	56	56	56
						57
					58	58
						59
				60	60	60
						61
					62	62
						63
64	64	64	64	64	64	64
						65
					66	66
						67
				68	68	68
						69
					70	70
						71
			72	72	72	72
						73
					74	74
						75
				76	76	76
						77
					78	78
						79
		80	80	80	80	80
						81
					82	82
						83
				84	84	84
						85

						86	86
							87
				88	88	88	88
							89
						90	90
							91
					92	92	92
							93
						94	94
							95
		96	96	96	96	96	96
							97
						98	98
							99
					100	100	100
							101
						102	102
							103
				104	104	104	104
							105
						106	106
							107
					108	108	108
							109
						110	110
							111
			112	112	112	112	112
							113
						114	114
							115
					116	116	116
							117
						118	118
							119
				120	120	120	120
							121
						122	122
							123
					124	124	124
							125
						126	126
							127
128	128	128	128	128	128	128	128
							129
						130	130
							131
					132	132	132
							133

				134	134
					135
			136	136	136
					137
				138	138
					139
				140	140
					141
				142	142
					143
		144	144	144	144
					145
				146	146
					147
				148	148
					149
				150	150
					151
			152	152	152
					153
				154	154
					155
				156	156
					157
				158	158
					159
	160	160	160	160	160
					161
				162	162
					163
				164	164
					165
				166	166
					167
			168	168	168
					169
				170	170
					171
				172	172
					173
				174	174
					175
		176	176	176	176
					177
				178	178
					179
				180	180
					181

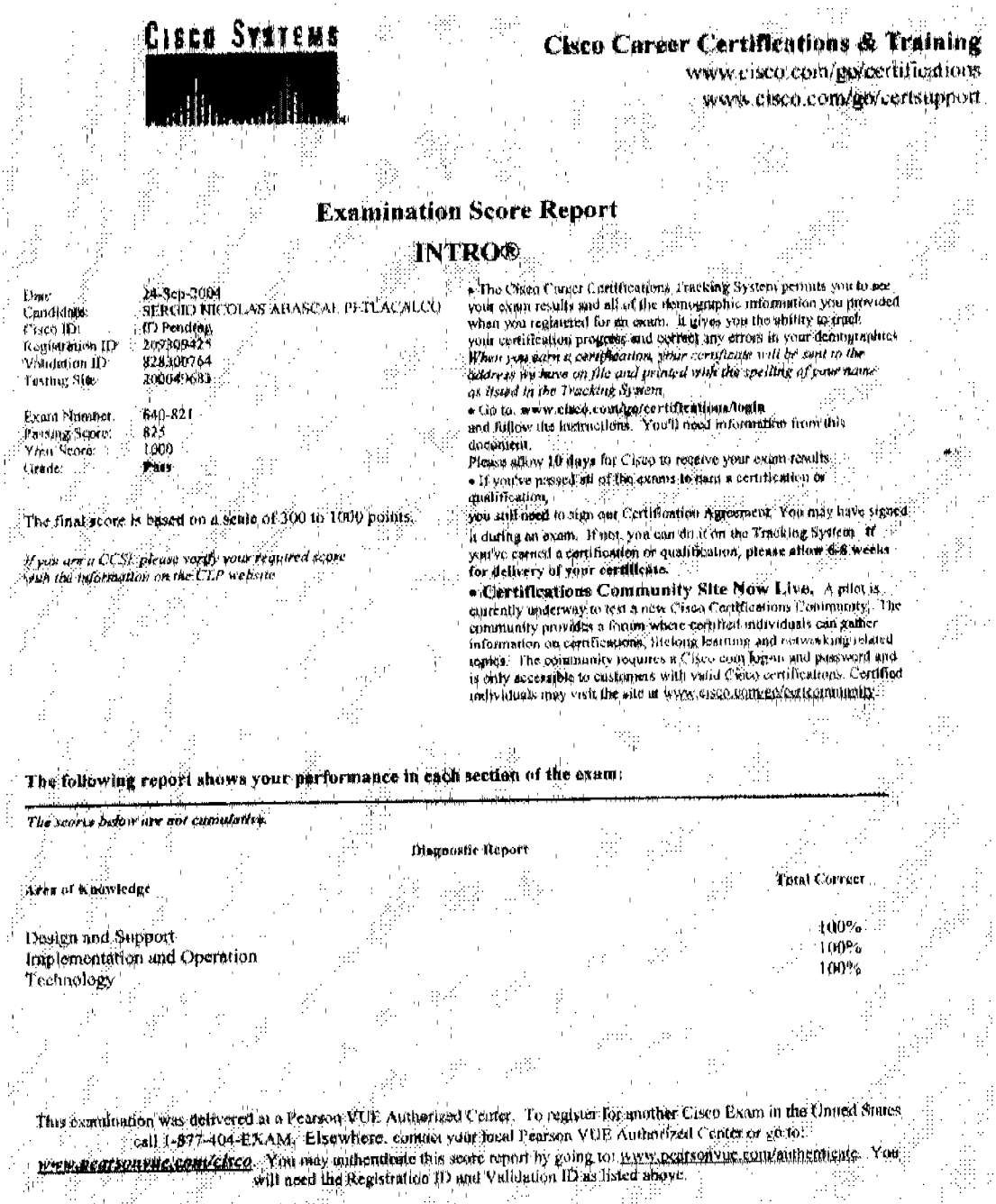
					182	182
						183
				184	184	184
						185
					186	186
						187
					188	188
						189
					190	190
						191
					192	192
192	192	192	192	192		193
					194	194
						195
					196	196
						197
					198	198
						199
				200	200	200
						201
					202	202
						203
					204	204
						205
					206	206
						207
			208	208	208	208
						209
					210	210
						211
					212	212
						213
					214	214
						215
				216	216	216
						217
					218	218
						219
					220	220
						221
					222	222
						223
		224	224	224	224	224
						225
					226	226
						227
					228	228
						229

						230	230
							231
				232	232	232	232
							233
						234	234
							235
					236	236	236
							237
						238	238
							239
			240	240	240	240	240
							241
						242	242
							243
					244	244	244
							245
						246	246
							247
				248	248	248	248
							249
						250	250
							251
					252	252	252
							253
						254	254
							255
256	256	256	256	256	256	256	256

Apéndice B

Resultados del Examen Obtenidos con la Ayuda de este Material.

Agradezco a mis estimados alumnos, quienes utilizaron por primera vez este método y les felicito por el logro alcanzado.



Cisco Systems

Cisco Career Certifications & Training
www.cisco.com/go/certifications
www.cisco.com/go/certsupport

Examination Score Report

INTRO®

Date:	24-Sep-2004
Candidate:	SERGIO NICOLAS ABASCAL PETLACALCO
Cisco ID:	(0 Pending)
Registration ID:	209309425
Validation ID:	928300764
Testing Site:	200049683
Exam Number:	640-821
Passing Score:	825
Your Score:	1000
Grade:	**Pass**

The final score is based on a scale of 300 to 1000 points.

If you are a CCSI please verify your required score with the information on the CLP website

- The Cisco Career Certifications Tracking System permits you to see your exam results and all of the demographic information you provided when you registered for an exam. It gives you the ability to track your certification progress and correct any errors in your demographics. *When you earn a certification, your certificate will be sent to the address you have on file and printed with the spelling of your name as listed in the Tracking System.*
- Go to: **www.cisco.com/go/certifications/login** and follow the instructions. You'll need information from this document.

Please allow 10 days for Cisco to receive your exam results.

- If you've passed all of the exams to earn a certification or qualification, you still need to sign our Certification Agreement. You may have signed it during an exam. If not, you can do it on the Tracking System. If you've earned a certification or qualification, **please allow 6-8 weeks for delivery of your certificate.**
- **Certifications Community Site Now Live.** A pilot is currently underway to test a new Cisco Certifications Community. The community provides a forum where certified individuals can gather information on certifications, lifelong learning and networking related topics. The community requires a Cisco.com logon and password and is only accessible to customers with valid Cisco certifications. Certified individuals may visit the site at www.cisco.com/go/certcommunity.

The following report shows your performance in each section of the exam:

The scores below are not cumulative.

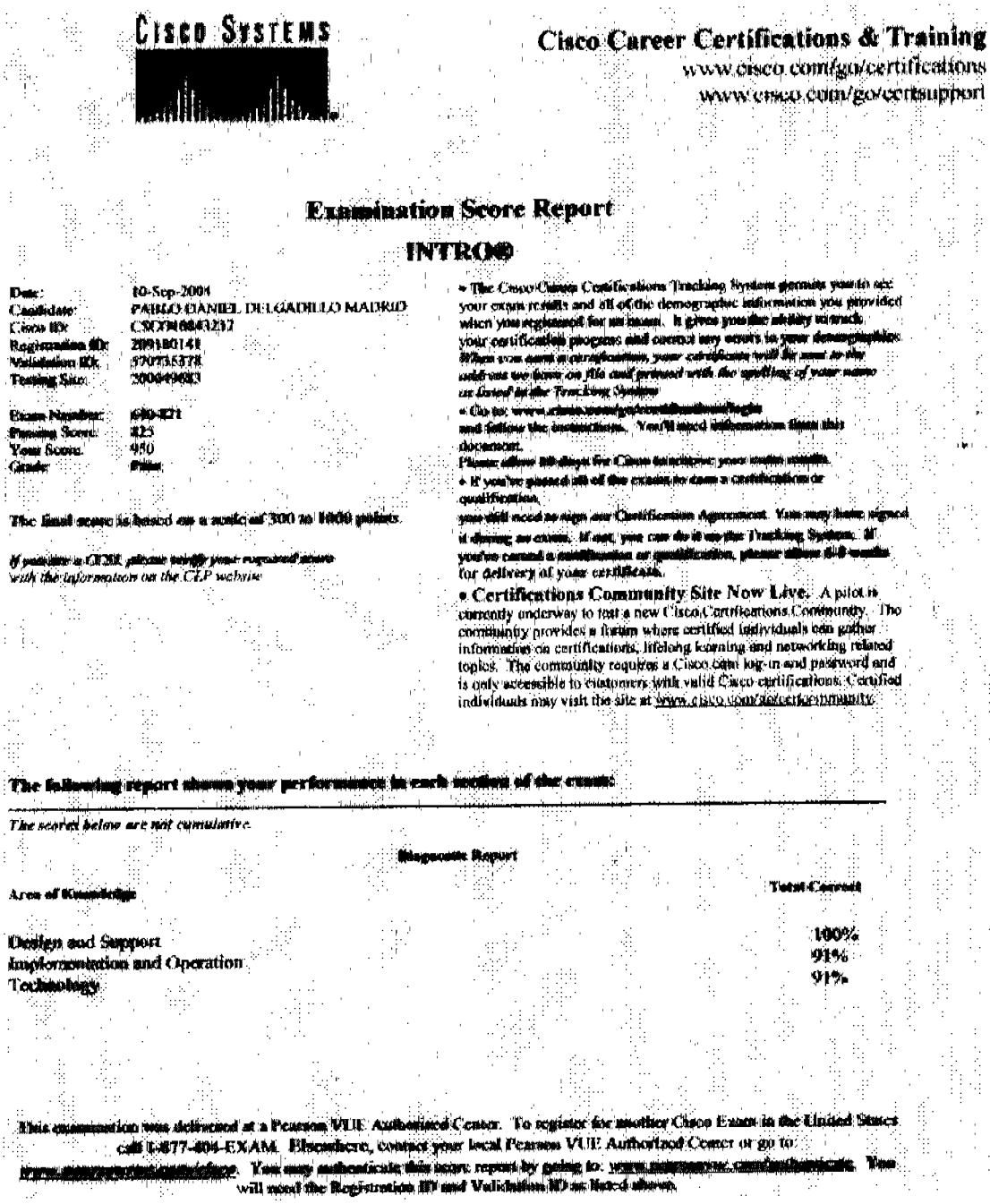
Diagnostic Report

Area of Knowledge	Total Correct
Design and Support	100%
Implementation and Operation	100%
Technology	100%

This examination was delivered at a Pearson VUE Authorized Center. To register for another Cisco Exam in the United States call 1-877-404-EXAM. Elsewhere, contact your local Pearson VUE Authorized Center or go to: www.pearsonvue.com/cisco. You may authenticate this score report by going to: www.pearsonvue.com/authenticate. You will need the Registration ID and Validation ID as listed above.

¡El método de estudio es sorprendente! Los conceptos se entienden de forma natural y los ejemplos lo hacen muy ameno. Realmente lo recomiendo altamente; sin él no hubiera logrado esta calificación (1000.)

-Ing. Sergio Abascal.



CISCO SYSTEMS

[redacted]

Cisco Career Certifications & Training
www.cisco.com/go/certifications
www.cisco.com/go/certsupport

Examination Score Report

INTRO00

Date: 10-Sep-2004
Candidate: PABLO DANIEL DELGADILLO MADRID
Cisco ID: CSCO10843237
Registration ID: 209180141
Validation ID: 370735378
Testing Site: 2000419083

Exam Number: 640-821
Passing Score: 825
Your Score: 950
Grade: Pass

The final score is based on a scale of 300 to 1000 points.

If possible, a CERF, please verify your supplied name with the information on the CEP website

- The Cisco Career Certifications Tracking System permits you to see your exam results and all of the demographic information you provided when you registered for an exam. It gives you the ability to track your certification progress and correct any errors in your demographics. *When you earn a certification, your certificate will be sent to the valid one we have on file and printed with the spelling of your name as listed in the Tracking System.*
- Go to: www.cisco.com/go/certifications/login and follow the instructions. You'll need information from this document.
Please allow 8-10 days for Cisco to receive your exam results.
- If you've passed all of the exams for exam a certification or qualification, you still need to sign our Certification Agreement. You may have signed it during an exam. If not, you can do it via the Tracking System. If you've earned a certification or qualification, please allow 4-6 weeks for delivery of your certificate.
- **Certifications Community Site Now Live.** A pilot is currently underway to test a new Cisco Certifications Community. The community provides a forum where certified individuals can gather information on certifications, lifelong learning and networking related topics. The community requires a Cisco.com log-in and password and is only accessible to customers with valid Cisco certifications. Certified individuals may visit the site at www.cisco.com/go/certcommunity

The following report shows your performance in each section of the exam:

The scores below are not cumulative.

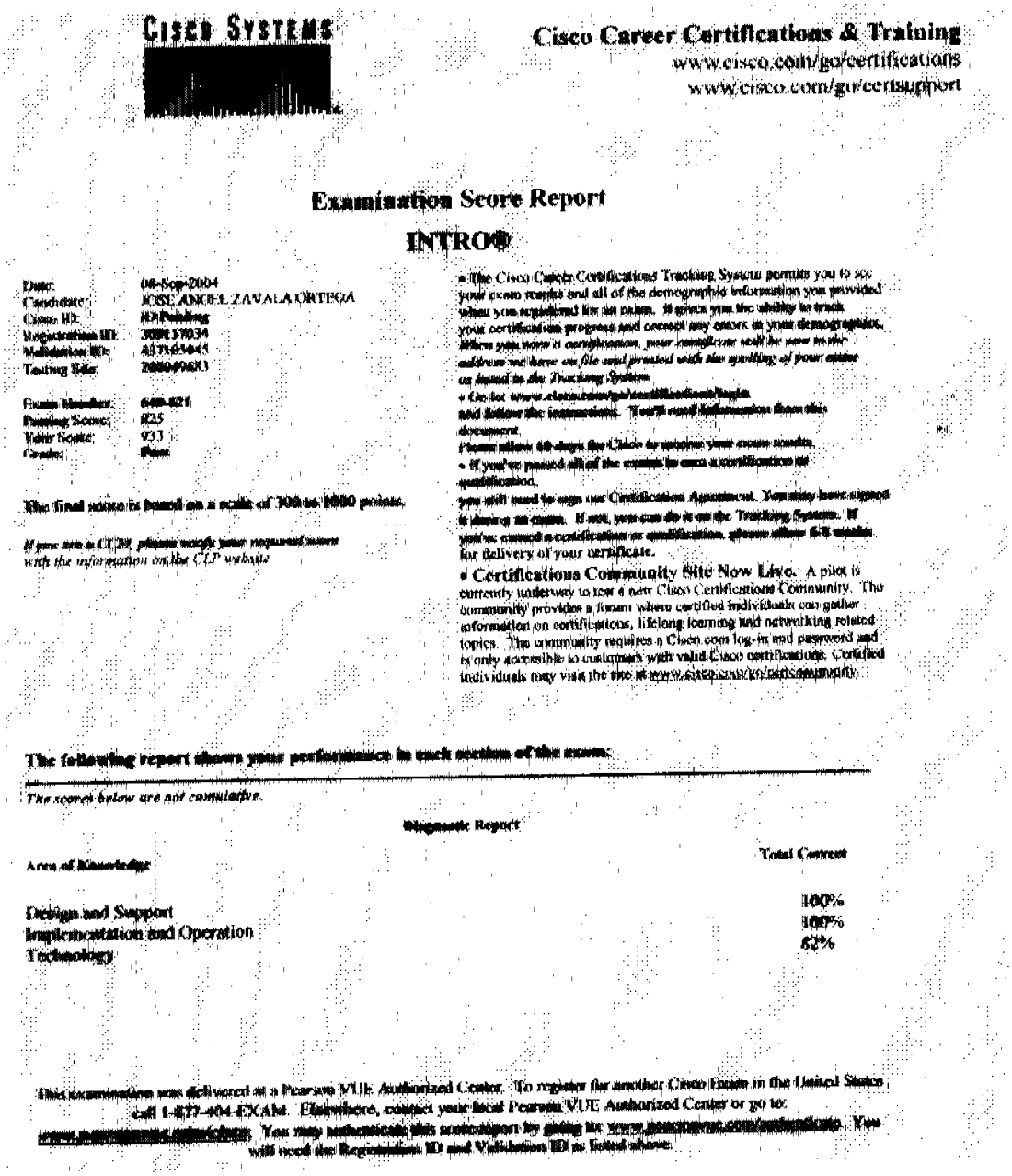
Diagnostic Report

Area of Knowledge	Total Correct
Design and Support	100%
Implementation and Operation	91%
Technology	91%

This examination was delivered at a Pearson VUE Authorized Center. To register for another Cisco Exam in the United States call 1-877-404-EXAM. Elsewhere, contact your local Pearson VUE Authorized Center or go to: [redacted]. You may authenticate this score report by going to: [redacted]. You will need the Registration ID and Validation ID as listed above.

El método de enseñanza me ha permitido adquirir conocimiento además de buenos resultados, debido a que he aprobado mis exámenes. El método resulta ser muy efectivo.

-Ing. Pablo Daniel Delgadillo



CISCO SYSTEMS

Cisco Career Certifications & Training
www.cisco.com/go/certifications
www.cisco.com/go/certsupport

Examination Score Report

INTRO®

Date: 06-Sep-2004
Candidate: JOSE ANGEL ZAVALA ORTEGA
Cisco ID: [redacted]
Registration ID: [redacted]
Validation ID: [redacted]
Testing Site: [redacted]

Exam Number: 640-821
Passing Score: 825
Your Score: 933
Grade: Pass

The final score is based on a scale of 300 to 1000 points.

If you are a CCIE, please notify your regional team with the information on the CCIE website

- The Cisco Career Certifications Tracking System permits you to see your exam results and all of the demographic information you provided when you registered for an exam. It gives you the ability to track your certification progress and correct any errors in your demographics. When you move to certification, your completion will be sent to the address we have on file and printed with the spelling of your name as found in the Tracking System.
- Go to: www.cisco.com/go/certifications/login and follow the instructions. You'll need information from this document.

Please allow 48 days for Cisco to process your exam results.

- If you've passed all of the exams to earn a certification or qualification, you will need to sign our Certification Agreement. You may have signed it during an exam. If not, you can do it on the Tracking System. If you've earned a certification or qualification, please allow 6-8 weeks for delivery of your certificate.
- **Certifications Community Site Now Live.** A pilot is currently underway to test a new Cisco Certifications Community. The community provides a forum where certified individuals can gather information on certifications, lifelong learning and networking related topics. The community requires a Cisco.com log-in and password and is only accessible to customers with valid Cisco certifications. Certified individuals may visit the site at www.cisco.com/go/certscommunity

The following report shows your performance in each section of the exam:

The scores below are not cumulative.

Diagnostic Report

Area of Knowledge	Total Correct
Design and Support	100%
Implementation and Operation	100%
Technology	82%

This examination was delivered at a Pearson VUE Authorized Center. To register for another Cisco Exam in the United States call 1-877-404-EXAM. Elsewhere, contact your local Pearson VUE Authorized Center or go to: [redacted]. You may authenticate this score report by going to: www.pearsonvue.com/authenticate. You will need the Registration ID and Validation ID as listed above.

He presentado dos exámenes utilizando el método de Raúl, ambos los he aprobado con resultados casi perfectos; el método no solamente me permitió aprobar mis exámenes, sino también adquirir una amplia capacitación técnica en aspectos relacionados.

-Ing. Jose Angel Zavala

Cisco Career Certifications & Training
www.cisco.com/go/certifications
www.cisco.com/go/certsupport

Examination Score Report

INTRO®

Date:	05-Jul-2004
Candidate:	JOSE LUIS NAVA RAMIREZ
Cisco ID:	ID Pending
Registration ID:	208770172
Validation ID:	1398260975
Testing Site:	20004963
Exam Number:	640-821
Passing Score:	825
Your Score:	916
Grade:	Pass

The final score is based on a scale of 300 to 1000 points.

If you are a CCSI, please verify your required score with the information on the CLP website

- The Cisco Career Certifications Tracking System permits you to see your exam results and all of the demographic information you provided when you registered for an exam. It gives you the ability to track your certification progress and correct any errors in your demographics. *When you earn a certification, your certificate will be sent to the address we have on file and printed with the spelling of your name as listed in the Tracking System.*
- Go to: www.cisco.com/go/certifications/login and follow the instructions. You'll need information from this document.
  Please allow 10 days for Cisco to receive your exam results.
- If you've passed all of the exams to earn a certification or qualification, you still need to sign our Certification Agreement. You may have signed it during an exam. If not, you can do it on the Tracking System. If you've earned a certification or qualification, *please allow 6-8 weeks for delivery of your certificate.*
- **Certification Community Site Now Live.** A pilot is currently underway to test a new Cisco Certifications Community. The community provides a forum where certified individuals can gather information on certification, lifelong learning and networking around topics. The community requires a Cisco.com log-in and password and is only accessible to customers with valid Cisco certifications. Certified individuals may visit the site at www.cisco.com/go/certcommunity

The following report shows your performance in each section of the exam:

The scores below are not cumulative.

Diagnostic Report

Area of Knowledge	Total Correct
Design and Support	100%
Implementation and Operation	100%
Technology	78%

This examination was delivered at a Pearson VUE Authorized Center. To register for another Cisco Exam in the United States call 1-877-404-EXAM. Elsewhere, contact your local Pearson VUE Authorized Center or go to: [redacted]. You may authenticate this score report by going to: www.pearsonvue.com/authenticate. You will need the Registration ID and Validation ID as listed above.

He probado el método de enseñanza y me parece una manera excelente para la capacitación técnica. Los resultados obtenidos son ampliamente satisfactorios.

Ing. José Luis Nava

Cisco Career Certifications & Training
www.cisco.com/go/certifications
www.cisco.com/go/certsupport

Beta Examination Score Report

INTRO

Date:	04-Feb-2004
Candidate:	JARET GARCIA SANCHEZ
Candidate ID:	CSCO10762997
Cisco ID:	CSCO10762997
Registration ID:	207965247
Validation ID:	1787033003
Testing Site:	200049683
Exam Number:	641-821
Passing Score:	867
document.	
Your Score:	933
Grade	**Pass**

qualification.
The final score is based on a scale of 300 to 1000 points.

If you are a CCSI, please verify your required score with the information on the CLP website

- The Cisco Career Certifications Tracking System permits you to see your exam results and all of the demographic information you provided when you registered for an exam. It gives you the ability to track your certification progress and correct any errors in your demographics. *When you earn a certification, your certificate will be sent to the address we have on file and printed with the spelling of your name as listed in the Tracking System*
- Go to: **www.cisco.com/go/certifications/login** and follow the instructions. You'll need information from this

Please allow **10 days** for Cisco to receive your exam results.
- If you've passed all of the exams to earn a certification or

you still need to sign our Certification Agreement. You may have signed it during an exam. If not, you can do it on the Tracking System. If you've earned a certification or qualification, **please allow 4-8 weeks for delivery of your certificate.**

The following report shows your performance in each section of the exam:

This beta exam contains new content and is in final stages of development. Unlike other Cisco beta exams, a "score report" has been provided with a final pass or fail determination at the end of the exam. Thank you for your participation in this beta exam and your contribution to the beta exam process.

The scores below are not cumulative.

Diagnostic Report

Area of Knowledge	Total Correct
Design and Support	100%
Implementation and Operation	100%
Technology	83%

This examination was delivered at a Pearson VUE Authorized Center. To register for another Cisco Exam in the United States call
1-877-404-EXAM. Elsewhere, contact your local Pearson VUE Authorized Center or go to: www.pearsonvue.com/cisco.

Raúl tiene una forma de volver los conceptos difíciles en fáciles de entender, me alegra que se haya decidido a poner su método por escrito.

-Ing. Jaret García

CISCO SYSTEMS

Cisco Career Certifications & Training
www.cisco.com/go/certifications
www.cisco.com/go/certsupport

Beta Examination Score Report

INTRO

Date:	03-Feb-2004
Candidate:	Octavio Carrera Castanon
Candidate ID:	CSCO10760917
Cisco ID:	CSCO10760917
Registration ID:	207965219
Validation ID:	1235443664
Testing Site:	20004968
Exam Number:	641-821
Passing Score:	867
document	
Your Score:	960
Grade:	**Pass**
qualification,	

The final score is based on a scale of 300 to 1000 points.

If you are a CCSI, please verify your required score with the information on the CLP website

• The Cisco Career Certifications Tracking System permits you to see your exam results and all of the demographic information you provided when you registered for an exam. It gives you the ability to track your certification progress and correct any errors in your demographics. *When you earn a certification, your certificate will be sent to the address we have on file and printed with the spelling of your name as listed in the Tracking System*

• Go to: www.cisco.com/go/certifications/login and follow the instructions. You'll need information from this

Please allow **10 days** for Cisco to receive your exam results.

• If you've passed all of the exams to earn a certification or

you still need to sign our Certification Agreement. You may have signed it during an exam. If not, you can do it on the Tracking System. If you've earned a certification or qualification, **please allow 6-8 weeks** for delivery of your certificate.

The following report shows your performance in each section of the exam:

This beta exam contains new content and is in final stages of development. Unlike other Cisco beta exams, a "score report" has been provided with a final pass or fail determination at the end of the exam. Thank you for your participation in this beta exam and your contribution to the beta exam process.

The scores below are not cumulative.

Diagnostic Report

Area of Knowledge	Total Correct
Design and Support	100%
Implementation and Operation	100%
Technology	90%

This examination was delivered at a Pearson VUE Authorized Center. To register for another Cisco Exam in the United States call

1-877-404-EXAM. Elsewhere, contact your local Pearson VUE Authorized Center or go to: www.pearsonvue.com/cisco

El material es muy bueno y conciso, con las lecturas breves y los ejemplos dados se tiene una mejor comprensión de los conceptos que en otros materiales. ¡Lo recomiendo ampliamente!

-Ing. Octavio Carrera

Glosario

A+ Certificación internacional ofrecida por CompTIA con la que se avala el dominio del *hardware* y *software* orientados a la configuración y mantenimiento de equipos de cómputo.

Access point Dispositivo utilizado para proveer conectividad a dispositivos móviles inalámbricos con la red alambrada.

Acknowledgment Mensaje enviado por un dispositivo a otro en la red, normalmente un dispositivo receptor lo envía para indicar que ha recibido correctamente un paquete.

ANSI *American National Standards Institute.* Organización estadounidense que norma la creación de estándares para la industria de las comunicaciones y computación.

APIPA *Automatic Private IP Addressing.* Cuando un sistema operativo esta configurado para obtener automáticamente los parámetros de la tarjeta de red (principalmente el IP), pero no encuentra el servidor DHCP, entonces se auto asigna una IP en el rango 169.254.0.0 con máscara 255.255.0.0.

Apple Talk Conjunto de protocolos de comunicación creados por Macintosh para uso en computadoras Apple.

ARCnet Estándar para interconexión de redes obsoleto, utilizaba cable coaxial RG-62.

ARP *Address Resolution Protocol.* Protocolo que relaciona la dirección lógica con la dirección física de un dispositivo. Dada una IP, ARP resuelve el MAC (no al reves.) ARP se define en el RFC 826.

AUI *Attachment Unit Interfase.* Conector tipo DB15 utlilizado en *hubs*, *switches* y ruteadores antiguos.

Backoff Algorithm Algoritmo de tiempo de espera que entra en acción cuando ocurre una colisión de *Frames* en una red *Ethernet.*

Beacon Un paquete muy ligero que se utiliza para monitorear el estado de una red *Token ring* o FDDI.

BNC *British Naval Connector, Bayonet Nelly Concelman* o *Bayonet Nut Connector.* Conector utilizado para cable coaxial delgado.

Bridge Dispositivo capaz de filtrar paquetes entre dos redes basándose en el MAC de destino. El *bridge*, al igual que el *switch* tiene un dominio de colisión en cada uno de sus puertos. La diferencia entre un *bridge* y un *switch* es que el *bridge* filtra por *software* mientras que el *switch* filtra por *hardware*, además del numero de puertos.

Broadcast Tipo de comunicación en la que el paquete se dirige a todos los dispositivos en el segmento visible. Se le reconoce por estar constituido solamente por unos en la dirección física o solamente unos en la parte de *host* de la dirección lógica.

Buffering Método de control de flujo en el que se cuida de no saturar el buffer de la tarjeta de red del receptor.

CCIE *Cisco Certified Internetwork Expert.* La certificación más robusta ofrecida por Cisco.

CCNA *Cisco Certified Network Asociate.*

CCNP *Cisco Certified Network Profesional.*

CDDI *Copper Distributed Data Interfase.* Implementación equivalente a FDDI pero con par trenzado en lugar de fibra óptica.

CDP *Cisco Discovery Protocol.* Protocolo creado por Cisco para determinar las características de los dispositivos directamente conectados al dispositivo local.

CIDR *Classless Inter-Domain Routing.* Método de manejo de redes en el cual se toman *bit*s correspondientes a la parte de *host* de un IP para convertirlos en sub-red.

Cisco fusion Un esfuerzo de Cisco para que todos sus dispositivos reconozcan los mismos comandos básicos sin importar la versión del sistema operativo.

Classfull Adjetivo que indica que solamente se pueden manejar redes considerando su máscara predeterminada por la clase a la que éstas pertenecen.

Classless Capacidad de manejar redes considerando sus máscaras de sub-red sin limitarse a las máscaras por clase a la que pertenecen las redes.

CLI *Command Line Interface.* Permite configurar dispositivos Cisco por medio de la línea de comandos.

CompTIA *The Computing Technology Industry Association.* Asociación no lucrativa y sin nexos comerciales que establece estándares a la comunidad tecnológica en la industria de la computación.

CRC *Cyclic Redundancy Check.* Método de detección de errores en el que el emisor divide el contenido de un *Frame* entre un número primo y anexa el residuo al *Frame.* Al llegar al receptor, se hace el mismo cálculo y se compara el residuo obtenido contra el que se obtuvo al enviar el *Frame.*

Crossover cable Tipo de cable de par trenzado que se utiliza para conectar dispositivos iguales entre sí, y que se caracteriza por cruzar algunas de las líneas entre los extremos del cable.

Crosstalk Error provocado por la interferencia que se producen mutuamente los campos electromagnéticos de líneas que corren juntas.

CSMA/CA *Carrier Sense Múltiple Access with Collision Avoidance.* Método de acceso en el que las computadoras que quieren transmitir emiten primero un paquete muy ligero en el que sólo expresan su deseo de transmitir. De esa manera se evitan las colisiones en los paquetes de información.

CSMA/CD *Carrier Sense Múltiple Access with Collision Detection.* Tecnología definida por el estándar IEEE 802.3 en el que los dispositivos escuchan el medio y reciben todo paquete que se ponga en él para determinar si son el destinatario o no. En este método, sólo una computadora puede utilizar el medio a la vez.

CSU/DSU *Channel Service Unit / Digital Service Unit.* Dispositivo de la capa física que convierte una señal tipo LAN a una tipo WAN.

Cut-through Técnica por la cual un *switch* envía un *Frame* que ha recibido hacia su destino tan pronto lee la dirección del destinatario en el *Frame.*

Checksum Número calculado para asegurar la integridad de un dato transmitido. Éste se calcula por medio de funciones matemáticas en ambos extremos de la transmisión y se compara en el extremo receptor para determinar si el *Frame* recibido sufrió alteraciones en su trayecto.

Datagrama Unidades de información transmitidas sin establecer primero un circuito virtual.

DCE *Data Communications Equipment.* Extremo de la liga entre dos equipos en red que se encarga de proveer los parámetros de sincronía, como la frecuencia de reloj, para la comunicación. Generalmente más cercano a la capa de *core* del modelo jerárquico de Cisco que el otro equipo en la misma línea.

DHCP *Dynamic Host Configuration Protocol.* Protocolo que permite la asignación automática de parámetros de conexión a computadoras. Estos parámetros incluyen IP, máscara de red, puerta de salida y DNS.

Distancia administrativa Valor numérico que indica la prioridad en que un ruteador debe considerar las rutas obtenidas por distintos protocolos o medios. Cada protocolo o medio tiene una diferente distancia administrativa dependiendo de su confiabilidad. La fuente más confiable tiene una distancia administrativa de 0 mientras que la menos confiable de 255.

DNS *Domain Name Service.* Servicio de resolución automática de nombres de dominio a IP's.

DoD *Department of Defense.* Modelo TCP/IP. Creado por el departamento de la defensa de estados Unidos para asegurar la intercomunicación en red en caso de un evento devastador.

DTE *Data Terminal Equipment.* Equipo de comunicaciones o de cómputo en el extremo normalmente utilizado por el cliente en una enlace. Este equipo no provee los parámetros de sincronía que se seguirán en la comunicación. Véase DCE.

Duplex Forma de comunicación en la que, se utilizan dos canales para la transmisión; uno en cada sentido. En las comunicaciones *full duplex* se puede recibir y transmitir información simultáneamente.

EEPROM *Electronically Erasable Programmable Read-only Memory.* Circuito integrado de memoria que puede ser borrado y reprogramado electrónicamente.

EIA/TIA *Electronics Industries Association / Telecommunications Industries Association.*

EIGRP *Enhanced Interior Gate Routing Protocol.* Protocolo híbrido propietario de Cisco que combina características de los protocolos de ruteo por vector de distancia y de estado de ligas (*link state.*)

EMI *Electro Magnetic Interference.* Interferencia electromagnética que produce efectos no deseados sobre una transmisión.

Encapsulamiento Técnica en la cual las unidades de información de una capa superior en el modelo DoD se convierten en datos para la capa inmediata inferior en donde se le agrega un nuevo encabezado.

Encripción Método que se utiliza para revolver los *bit*s en la información que se envía con el fin de que cualquier intercepción maliciosa no represente una amenaza, ya que sin la clave de recuperación, y dependiendo del método de encripción, es prácticamente imposible leer la información.

FDDI *Fiber Distributed Data Interfase.* Estándar definido por la ANSI para la interconexión en una LAN que se implementa sobre un anillo doble de fibra óptica.

FDM *Frecuency Division Multiplexing.* Técnica para transmitir varias señales sobre el mismo medio físico asignándoles diferentes canales de frecuencia

Fibra monomodo Tipo de fibra óptica capaz de transportar una sola señal simultáneamente.

Fibra multimodo Tipo de fibra óptica capaz de transportar múltiples señales simultáneamente.

Firewall Filtro lógico que permite tener seguridad entre equipos interconectados. El firewall se basa en características del *Frame* para permitir o no el paso de éste al sistema de destino.

Flapping Término que describe a una interfase que se prende y apaga de manera frecuente por causas tales como un falso contacto.

Flooded broadcast Técnica en la que el datagrama recibido en una interfase se transmite a todas las demás interfases.

Flush La acción de desechar rutas de la tabla de ruteo.

FQDN *Fully Qualified Domain Name.* Forma de especificar los nombres tipo *hostname* en la que se aprecian todos los dominios y sub-dominios a los que pertenecen.

Fragment free Técnica de *switcheo* en la que el *switch* espera a recibir 64 *bytes* sin errores de colisión o interferencias antes de comenzar a enviar el datagrama al destino especificado en la MAC de destino. También se le conoce como Modified Cut Through.

Frame Relay Tipo de conexión WAN en la que se comparte el medio por varios usuarios a fin de abaratar el servicio. Cada usuario tiene un ancho de banda mínimo asegurado pero si la demanda lo permite, puede utilizar la totalidad del ancho de banda que permita el medio.

FTP *File Transfer Protocol.* Protocolo de TCP/IP que permite la transmisión de múltiples tipos de archivos por medio de la red.

Gateway Función que traduce formatos, protocolos, topologías, etc. entre redes dispares.

Half Duplex Tipo de comunicación en la que el medio de comunicación se utiliza en ambos sentidos pero no simultáneamente.

Holddown Tiempo de histéresis que permite que las entradas en las tablas de ruteo sean consistentes a pesar de aparentes mejoras que tan sólo duran algunos segundos.

Hop "Salto" de un datagrama al pasar por un ruteador.

Host Cualquier dispositivo direccionable desde la red.

Host ID Parte de la dirección lógica que identifica a un host en particular.

Hosts file Archivo que de manera estática relaciona la dirección lógica de un sitio o dispositivo con su *hostname*.

IANA *Internet Assigned Numbers Authority*. Organismo encargado de asignar IP's.

ICA *Independant Computing Architecture*. Modificación a Telnet que soporta el manejo de ambiente grafico y no es dependiente al fabricante del sistema en que se utilice.

ICMP *Internet Control Message Protocol*. Protocolo de TCP/IP que monitorea el estado de las conexiones entre dispositivos. Dos de sus comandos más conocidos son Ping y Traceroute.

ICS *Internet Connection Sharing*. Servicio que permite a un sistema cliente compartir una conexión a Internet.

IEEE *Institute of Electronical and Electronics Engineers*. Organización que define estándares en varios campos de la ingeniería.

IGMP *Internet Group Management Protocol*. Protocolo de TCP/IP que se utiliza para mandar un datagrama en *multicast*.

IGRP *Interior Gateway Routing Protocol*. Protocolo de vector de distancia desarrollado por Cisco que mejora muchas características ofrecidas por RIP.

IMAP *Internet Message Access Protocol*. Protocolo utilizado para el manejo de mensajería por Internet.

IOS *Internetwork Operating System*. Sistema operativo de los *switches* y ruteadores Cisco.

IP *Internet Protocol*. Dirección lógica en TCP/IP, compuesta de 32 *bits* normalmente expresados en notación decimal punteada y que especifica el *Net ID* y *Host* ID de un dispositivo.

IPX *Internet Packet Exchange.* Dirección lógica de Novel que se forma por 10 pares de dígitos hexadecimales y que contiene la MAC del dispositivo en el cual se asigna.

IRQ *Interruption Request.* Requisición de interrupción al sistema operativo para atender una solicitud de servicio que requiere tiempo del procesador.

ISO *International Standarization Organization.* Organización internacional de estándares. Creadora del modelo OSI.

ISP *Internet Service Provider.* Proveedor del servicio de Internet.

LAN *Local Area Network.* Red de área local.

LPD *Line Printer Daemon.* LPD es un protocolo diseñado para compartir impresoras. LPD se utiliza en conjunto con LPR (*Line Printer*) para imprimir por medio de la red utilizando TCP/IP como protocolo al enviar los documentos a imprimir.

LPR Véase LPD.

LLC *Logical Link Control.* Sub-capa de la capa de enlace de datos que controla el flujo de datos entre el emisor y el receptor en una comunicación.

MAC *Media Access Control.* Sub-capa de la capa de enlace de datos que direcciona de manera física los dispositivos.

MAN *Metropolitan Área Network.* Red que comprende un área metropolitana, comúnmente mayor que una LAN pero menor que una WAN.

Memoria Flash Tipo de memoria que permite almacenar, ejecutar y borrar imágenes de *software*. Cisco utiliza la memoria flash para almacenar y ejecutar el IOS de sus dispositivos.

Mesh Topología de red en la que cada dispositivo se conecta directamente a todos los demás dispositivos.

MSAU *Multi-Station Access Unit.* Concentrador que provee la secuenciación entre los dispositivos en una topología anillo.

MTU *Maximum Tansmission Units.* Tamaño máximo en *bytes* de las unidades de transmisión entre emisor y receptor en una comunicación, considerando los tamaños de sus buffers.

Multicast Tipo de transmisión que se hace con varios destinatarios miembros de una lista de suscripción.

NAT *Network Address Translation.* Servicio que permite a un datagrama en una red privada salir a Internet utilizando una IP publica "prestada".

Net ID Parte de la dirección lógica que identifica a la red o sub-red a la que pertenece un IP dado, según su máscara.

NetBIOS *Network Basic Input Output System.* Sistema desarrollado por IBM para el manejo de procesos de red a un nivel cercano al *hardware.*

NetWare Sistema Operativo de Red creado por Novel.

NFS *Network File System.* NFS es un protocolo que se especializa en permitir que dos sistemas de archivos que normalmente son incompatibles puedan transferir archivos entre ellos.

NMS *Network Management System.* NMS permite navegar por un mapa de la red y por medio del mouse obtener información o incluso establecer parámetros a cualquiera de los dispositivos que estén corriendo en ellos el agente SNMP.

NVRAM *Non Volatile RAM.* Memoria RAM que mantiene el contenido de sus celdas aún al apagar el dispositivo que la contiene.

OSI *Open Systems Interconnection.* Modelo de referencia que permite estandarizar por capas, las funciones que se deben realizar para que un datagrama pueda ser enviado por medio de una red.

OSPF *Open Shortest Path First.* Protocolo de ruteo de link-state (estado de ligas) que se basa en el ancho de banda para determinar la mejor ruta.

PDU *Protocol Data Unit.* Unidad de transmisión que tiene diferentes componentes y toma diferentes nombres según en la capa donde se encuentre.

Ping *Paket Internet Groper.* Herramienta de diagnostico de conectividad en redes. Ping envía una señal llamada *echo request* y espera recibir un *echo reply* para determinar si hay conectividad hacia un *host* de destino.

POP *Post Office Protocol.* Protocolo utilizado para recuperar el correo electrónico desde un servidor de correo.

POST *Power On Self Test.* Serie de pruebas que corre un ruteador al arrancar para determinar su propio estado de *hardware* y *software.*

Priviledged exec user mode Modo privilegiado de ejecución en un *switch* o ruteador Cisco, se reconoce por el indicador "#".

PROM *Programmable Read Only Memory.* Memoria que se puede programar por única vez.

RAM *Random Access Memory.* Memoria volátil que en los equipos Cisco almacena la configuración corriente, las tablas de ruteo, y los buffers de paquetes.

RARP *Reverse Address Resolution Protocol.* Protocolo de TCP/IP que relaciona una dirección de MAC dada a la correspondiente IP del *host* de destino.

RIP *Routing Information Protocol.* Protocolo de ruteo de vector de distancia que basa su métrica en la cuenta de hops (15 máximo.)

Setup mode Modo de configuración guiada al que entra un ruteador que no tiene una configuración de arranque válida o que la ha ignorado al arrancar.

Simplex Método de comunicación en el que el medio de transporte se utiliza en un solo sentido.

SMTP *Simple Mail Transfer Protocol.* Protocolo que provee servicios de correo electrónico para Internet.

SNMP *Simple Network Management Protocol.* Protocolo de manejo y monitoreo de la red.

Store and forward Técnica de *switcheo* en la que el *switch* espera a recibir el datagrama completo en buen estado antes de comenzar a enviarlo por el puerto que conduce al dispositivo de destino.

Straight-through Tipo de cable que se utiliza para conectar dispositivos de diferentes jerarquías; en especifico un *hub* con una computadora, un *switch* con una computadora, un ruteador con un *switch*, y un ruteador con un *hub*.

TCP *Transmission Control Protocol.* Protocolo de TCP/IP orientado a la conexión y confiable que se encuentra en la capa de transporte del modelo OSI.

TCP/IP *Transmission Control Protocol/Internet Protocol.* Conjunto de protocolos creado por el departamento de defensa de los Estados Unidos que enfatiza la seguridad de entrega en una transmisión. Es el conjunto de protocolos más utilizado hoy en día.

TDM *Time Division Multiplexing.* Multiplexión por división en el tiempo. En este método de transmisión, el medio se utiliza como varios canales, dividido en el tiempo.

Telnet Método de conexión remota que emula en una terminal, la línea de comandos del dispositivo remoto para manejarlo como si se estuviera frente a él.

TFTP *Trivial File Transfer Protocol.* Protocolo de transferencia de archivos basado en UDP.

Three Way Handshake "Apretón de manos de tres vías" Algoritmo que utiliza TCP para establecer una conexión antes de iniciar una comunicación.

Token passing Método de acceso al medio que utiliza la topología *Token Ring.* En este método, un *token* o estafeta circula para proveer una oportunidad de transmisión a cada uno de los dispositivos en el anillo.

Token ring Topología de red que asemeja un anillo. Puede ser implementada con un anillo físico o un anillo lógico sobre una estrella física.

Traceroute Uno de los comandos más utilizados de ICMP. Traceroute especifica la ruta que un paquiete de información sigue para llegar a su destino.

TTL El TTL es un número que se le agrega al paquete y se va decrementando con cada salto por un ruteador en la red.

UART *Universal Asynchronous Receiver/Transmitter.* Circuito integrado que se encarga de transformar los datos de una computadora para que se puedan transmitir por una interfase asíncrona.

UDP *User Datagram Protocol.* Protocolo no orientado a la conexión y no confiable de la capa de transporte del modelo DoD.

Unicast Tipo de transmisión en la que el paquete tiene un solo destinatario.

User Exec mode Modo de ejecución de usuario normal en un IOS de un ruteador o *switch* Cisco. Se reconoce por el indicador ">".

VFIR *Very Fast Infrared.* Estándar que define el uso de rayos infrarrojos para altas velocidades.

VLSM *Variable Length Subnet Masks.* Método para optimizar la asignación de IP's en una red al utilizar en cada segmento la máscara de sub-red más adecuada para ese segmento en particular sin importar que no sea igual para todos los segmentos.

WAN *Wide Área Network.* Red de área global. red extensa que normalmente interconecta varias LANs.

WAP *Wireless Access Point.* Dispositivo que permite la interconexión de dispositivos inalámbricos con una red alambrada.

Windowing Método de control de flujo que aprovecha el tiempo que tarda un *Frame* en alcanzar las capas superiores para enviar más *Frames*. El tamaño de la ventana especifica cuantos *Frames* se enviarán antes de esperar recibir un *Acknowledgment*.

WINS *Windows Internet Name Service.* Servicio de red que relaciona un IP a un nombre NetBIOS name dado.

Bibliografía

- Barkl, Andy. Cisco Certified Design Associate. 2003. Ed. SYBEX. ed. 2a.

- Heywood, Drew. Redes con Microsoft TCP/IP. 1998. Ed. Prentice Hall.

- McQuerry, Steve. Interconnecting Cisco Network Devices. 2000. Ed. Cisco Systems, Inc.

- Odom, Wendell. Cisco CCNA Exam #640-507 Certification Guide. 2001. Cisco Systems, Inc.

- Quiroz, Gerardo. Microsoft Fundamentos de Redes Plus. 1995. Ed. McGraw-Hill Interamericana de España.

- Sin autor. Microsoft Windows 2000 Network and Operating System Essentials. 2002. Ed. Cargvajal S.A. de C.V.