ES CISCO

Guía de estudio para la certificación CCNA 640-802

2ª EDICIÓN

zo por garantizar que los profesionales de las redes posean los conocimientos necesa- alizar las tareas de soporte y administración, Cisco Systems ha desarrollado una serie de rtificaciones que actúan como punto de referencia de las tecnologías de redes. Los le certificación están diseñados para superar las pruebas de habilidades teóricas y de ón de dispositivos en varias jerarquías. Las certificaciones Cisco son muy valoradas por s y van desde el nivel asociado **CCNA** (*Cisco Certified Network Associate*), el nivel profe- P (*Cisco Certified Network Professional*) hasta el nivel experto **CCIE** (*Cisco Certified k Expert*).

presenta una herramienta de autoestudio para el aprendizaje de los temas relacionados con del examen de certificación **CCNA 640-802**. Esta obra proporciona los conceptos, coman- as necesarias para configurar routers y switches Cisco para que funcionen en las redes y para alcanzar dicha certificación. Aunque este libro fue creado para aquellos que certificación CCNA, también es útil para administradores, personal de soporte o para los nente desean entender más claramente el funcionamiento de las LAN, las WAN, sus los servicios de acceso.

está dividido en diez capítulos bien definidos cumpliendo los objetivos del examen de CCNA, según el criterio y experiencia de su autor, con métodos claros y rápidos incluso lo de subredes, VLSM y Wildcards. Diseminados por el texto hay muchas notas, conse- arios que ayudan a la comprensión y memorización del temario.

ibro se incorporan apéndices complementarios con comandos Cisco IOS adicionales, milares a las que aparecen en el examen de certificación CCNA y un completo glosario inos mas usuales utilizados en redes.

volcado su amplia experiencia en este material y su trabajo en Europa y Latinoamérica ha le la creación de este libro no solo desde el punto de vista técnico, sino también desde . Su comprensión metódica y la complementación con prácticas harán, sin duda, llegar e al estudiante a la obtención de la tan valorada certificación CCNA, convirtiéndose ite en una guía de consulta permanente.

ganello es ingeniero de comunicaciones, instructor certificado de Cisco Networking Academy, imparte nados con redes y comunicaciones. Especialista en electrónica de hardware de alta complejidad. certificaciones, entre ellas el CCNP y CCAI. Es catedrático y consultor especializado en comunicaciones de diversos títulos entre ellos: *Redes Cisco. Guía de estudio para la certificación CCNP.*

omega.com.mx

ISBN 970-607-707-326-0

"Te acerca al conocimiento"

Ariganello

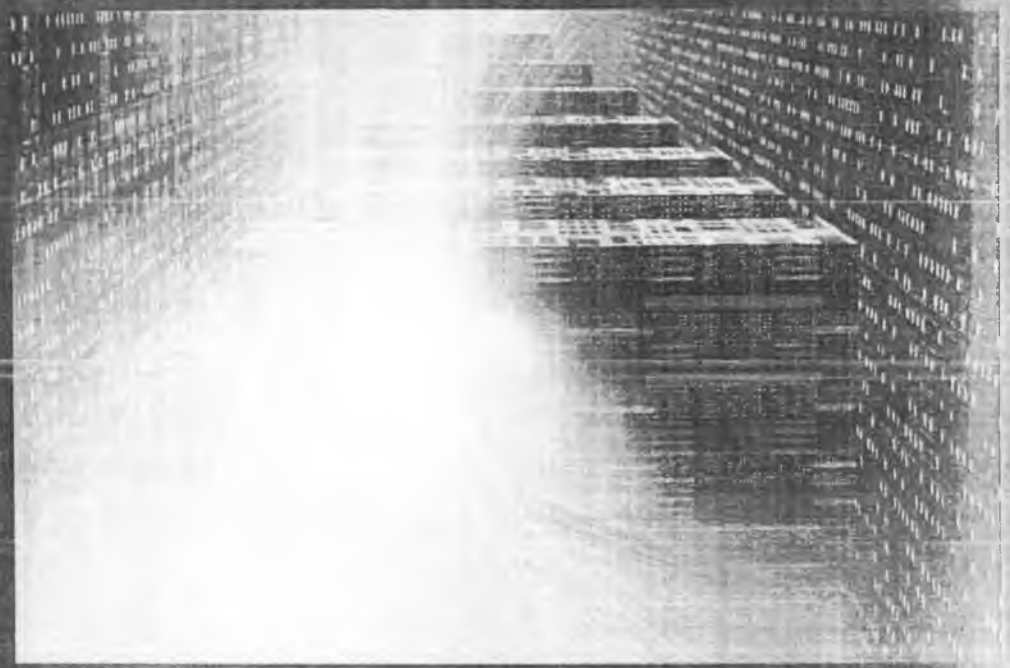
REDES CISCO

2ª EDICIÓN

REDES CISCO

Guía de estudio para la certificación CCNA 640-802

2ª EDICIÓN



Ernesto Ariganello

REDES CISCO

Guía de estudio para la certificación CCNA 640-802

2ª Edición

REDES CISCO

Guía de estudio para la certificación CCNA 640-802

2ª Edición

Ernesto Ariganello

Alfaomega Ra-Ma®

Datos catalográficos
Ariganello, Ernesto
Redes Cisco. Guía de estudio para la certificación CCNA 640-802
Segunda Edición
Alfaomega Grupo Editor, S.A. de C.V., México
ISBN: 978-607-707-326-0
Formato: 17 x 23 cm Páginas: 480

Redes Cisco. Guía de estudio para la certificación CCNA 640-802, 2ª Edición
Ernesto Ariganello
ISBN: 978-84-9964-094-5, edición original publicada por RA-MA Editorial, Madrid, España

Segunda edición: Alfaomega Grupo Editor, México, septiembre 2011

Pitágoras 1139, Col. Del Valle, 03100, México D.F.

Miembro de la Cámara Nacional de la Industria Editorial Mexicana
Registro No. 2317

Pág. Web: **http://www.alfaomega.com.mx**
E-mail: **atencionalcliente@alfaomega.com.mx**

ISBN: 978-607-707-326-0

Nota importante:
La información contenida en esta obra tiene un fin exclusivamente didáctico y, por lo tanto, no está previsto su aprovechamiento a nivel profesional o industrial. Las indicaciones técnicas y programas incluidos, han sido elaborados con gran cuidado por el autor y reproducidos bajo estrictas normas de control. ALFAOMEGA GRUPO EDITOR, S.A. de C.V. no será jurídicamente responsable por: errores u omisiones; daños y perjuicios que se pudieran atribuir al uso de la información comprendida en este libro, ni por la utilización indebida que pudiera dársele.

Edición autorizada para venta en México y todo el continente americano.

Impreso en México. Printed in Mexico.

Empresas del grupo:

México: Alfaomega Grupo Editor, S.A. de C.V. – Pitágoras 1139, Col. Del Valle, México, D.F. – C.P. 03100.
Tel.: (52-55) 5575-5022 – Fax: (52-55) 5575-2420 / 2490. Sin costo: 01-800-020-4396
E-mail: atencionalcliente@alfaomega.com.mx

Colombia: Alfaomega Colombiana S.A. – Carrera 15 No. 64 A 29, Bogotá, Colombia,
Tel.: (57-1) 2100122 – Fax: (57-1) 6068648 – E-mail: cliente@alfaomega.com.mx

Chile: Alfaomega Grupo Editor, S.A. – Dr. La Sierra 1437, Providencia, Santiago, Chile
Tel.: (56-2) 235-4248 – Fax: (56-2) 235-5786 – E-mail: agechile@alfaomega.cl

Argentina: Alfaomega Grupo Editor Argentino, S.A. – Paraguay 1307 P.B. Of. 11, C.P. 1057, Buenos Aires, Argentina, – Tel./Fax: (54-11) 4811-0887 y 4811 7183 – E-mail: ventas@alfaomegaeditor.com.ar

ÍNDICE

INTRODUCCIÓN

Este libro representa una herramienta de apoyo y de autoestudio para el aprendizaje de los temas y requisitos necesarios para lograr la certificación CCNA 640-802. Ha sido concebido como complemento a los diferentes materiales de capacitación que Cisco provee a sus alumnos como así también a aquellos que desean examinarse de manera independiente.

Debido a la idea práctica y concreta de este manual se dan por entendidos muchos temas básicos, por lo que es recomendable poseer algún conocimiento mínimo previo a la lectura de estas páginas.

Es importante que el alumno asimile y ejercite los contenidos de cada capítulo antes de seguir adelante con el siguiente. El libro tiene un formato secuencial y lógico de tal manera que permite seguir todos los temas en orden ascendente. Los apéndices finales contienen un listado de comandos Cisco IOS, una serie de recomendaciones para la presentación al examen y 400 preguntas similares a las que aparecen en la certificación CCNA, como apoyo y nivelación de conocimientos y un glosario con los términos más usados en redes.

El objetivo de este libro es instruir al lector acerca de las tecnologías del networking, configurar y entender el funcionamiento de los routers y switches no sólo con la finalidad de obtener la certificación CCNA sino también para aquellos que lo quieran utilizar como material de consulta. Está enfocado también para profesores e instructores que lo quieran emplear como apoyo para sus clases en centros de estudios o academias.

Las características de este libro ayudan a facilitar la comprensión de los temas presentados de manera resumida pero detallada con explicaciones, notas y llamadas para permitir que el lector recuerde lo fundamental y concreto a la hora de presentarse al examen de certificación. Los casos prácticos son ejemplos de ejercicios hechos en clase por el autor siendo muy recomendable que el lector los realice en equipos reales o en simuladores para su completa comprensión y análisis.

Las preguntas finales son ejemplos similares a las que aparecen en el examen de certificación CCNA 640-802, por tanto, es importante para lograr el éxito deseado, leerlas y analizarlas detenidamente buscando si fuese necesario la referencia en la página correspondiente hasta tener un completo dominio de cada tema.

Los libros de la serie REDES CISCO son un complemento a esta guía de estudio. Para aquellos que persiguen la certificación profesional de Cisco la *Guía de estudio para la certificación CCNP* y la *Guía de estudio para profesionales* serán sin duda el material necesario para obtener la certificación CCNP.

Editorial Alfaomega - RA-MA
ISBN: 978-607-707-182-2

Editorial Alfaomega - RA-MA
ISBN: 978-607-7854-79-1

Agradecimientos

Agradezco al lector por confiar en mi trabajo y por honrarme con su interés de aprender con este libro.

A todos los alumnos e instructores con los que he tenido el placer de trabajar todos estos años, de los cuales siempre he aprendido cosas, a todos ellos también va este agradecimiento.

A mis editores una vez más por confiar en mí, dándome la posibilidad de otra nueva publicación.

A mi familia, a mis compañeros de trabajo y a los amigos de Argentina y España por su apoyo constante, especialmente a los que la lejanía los hace aún más cercanos.

Por último y fundamentalmente a Elizabeth, mi esposa, luchadora incansable de la vida, y a mi hijo Germán, cuyos méritos superan con creces los deseados por cualquier padre; a ambos gracias por estar conmigo en los momentos más difíciles.

Ernesto Ariganello

Acerca del autor

Ernesto Ariganello es instructor certificado de la *Cisco Networking Academy*, imparte cursos relacionado con redes y comunicaciones. Especialista en electrónica de hardware de alta complejidad. Posee varias certificaciones, entre ellas el CCNP. Es, además, consultor especializado en comunicaciones de datos para varias empresas de la Unión Europea. Su trabajo en educación y formación es sumamente valorado en Europa y Latinoamérica, fundamentado en clases claras, dinámicas y muy prácticas, por donde han pasado más de 1.000 alumnos por diferentes centros de formación y empresas.

Ha editado varios libros de la serie REDES CISCO, de los cuales su primera obra *Guía de estudio para la certificación CCNA* y la *Guía de estudio para la certificación CCNP* son reconocidas como las pioneras con contenidos escritos íntegramente en español.

Advertencia

Se ha realizado el máximo esfuerzo para hacer de este libro una obra tan completa y precisa como sea posible, pero no se ofrece ninguna garantía implícita de adecuación a un fin en particular. La información se suministra "tal como está". Los autores no serán responsables ante cualquier persona o entidad con respecto a cualquier pérdida, daño o perjuicio que pudieran resultar emergentes de la información contenida en este libro.

Todos los términos mencionados en este libro que, según consta, pertenecen a marcas comerciales o marcas de servicios, se utilizan únicamente con fines educativos. No debe considerarse que la utilización de un término en este libro afecte la validez de cualquier marca comercial o de servicio.

Los conceptos, opiniones y gráficos expresados en este libro por los autores no son necesariamente los mismos que los de Cisco Systems, Inc.

Los iconos y topologías mostradas en este libro se ofrecen con fines de ejemplo y no representan necesariamente un modelo de diseño para redes.

Las configuraciones y salidas de los routers, switches y/o cualquier otro dispositivo se han tomado de equipos reales y se ha verificado su correcto funcionamiento. No obstante, cualquier error en la transcripción es absolutamente involuntario.

Capítulo 1

INTRODUCCIÓN A LAS REDES

1.1 CONCEPTOS BÁSICOS

Antes de comenzar la lectura de este libro el estudiante debe tener claros ciertos conceptos que harán posible la mejor comprensión de cada uno de los temas descritos en estas páginas. Esta guía de estudio apunta principalmente a la certificación CCNA, profundizando en el temario cada vez más en cada capítulo. Estos primeros párrafos servirán como base a todo lo que sigue posteriormente.

Las infraestructuras de red pueden variar dependiendo del tamaño del área, del número de usuarios conectados y del número y los diferentes tipos de servicios disponibles. Además del dispositivo final, hay otros componentes que hacen posible que se establezca el enlace entre los dispositivos de origen y destino. Uno de los componentes críticos en una red de cualquier tamaño es el router, de la misma forma que el switch, el funcionamiento y configuración de ambos se detallarán en los capítulos siguientes.

Todos los tipos de mensajes se tienen que convertir a bits, señales digitales codificadas en binario, antes de enviarse a sus destinos. Esto es así sin importar el formato del mensaje original. Generalmente, las redes utilizan cables para proporcionar conectividad. Ethernet es la tecnología de red más común en la actualidad. Las redes cableadas son ideales para transmitir grandes cantidad de datos a altas velocidades. Las redes inalámbricas permiten el uso de dispositivos conectados a la red en cualquier lugar de una oficina o casa, incluso en el exterior.

Las redes de área local y las redes de área amplia, es decir las LAN y las WAN conectan a los usuarios dentro y fuera de la organización. Permiten gran cantidad y tipos de comunicación.

Sin embargo, los aspectos más importantes de las redes no son los dispositivos ni los medios, sino los protocolos que especifican la manera en que se envían los mensajes, cómo se direccionan a través de la red y cómo se interpretan en los dispositivos de destino.

1.2 MODELO DE REFERENCIA OSI

A principios de los años ochenta los fabricantes informáticos más importantes de la época se reúnen para unificar diferencias y recopilar la mayor información posible acerca de cómo poder integrar sus productos hasta el momento no compatibles entres sí y exclusivos para cada uno de ellos. Como resultado de este acuerdo surge el modelo de referencia **OSI**, que sigue los parámetros comunes de hardware y software haciendo posible la integración multifabricante.

El modelo OSI (modelo abierto de internetwork, no confundir con ISO) divide a la red en diferentes capas con el propósito de que cada desarrollador trabaje específicamente en su campo sin tener necesidad de depender de otras áreas. Un programador crea una aplicación determinada sin importarle cuáles serán los medios por los que se trasladarán los datos, inversamente un técnico de comunicaciones proveerá comunicación sin importarle qué datos transporta.

7	APLICACIÓN
6	PRESENTACIÓN
5	SESIÓN
4	TRANSPORTE
3	RED
2	ENLACE DE DATOS
1	FÍSICA

Las siete capas del modelo OSI

En su conjunto, el modelo OSI se compone de siete capas bien definidas que son: Aplicación, Presentación, Sesión, Transporte, Red, Enlace de Datos y Física.

Cada una de estas capas presta servicio a la capa inmediatamente superior, siendo la capa de aplicación la única que no lo hace ya que al ser la última capa su servicio está directamente relacionado con el usuario. Así mismo, cada una de estas siete capas del host origen se comunica directamente con su similar en el host de destino. Las cuatro capas inferiores también son denominadas capas de Medios (en algunos casos capas de Flujo de Datos), mientras que las tres superiores capas se llaman de Host o de Aplicación.

Modelo OSI:

- Proporciona una forma de entender cómo operan los dispositivos en una red.
- Es la referencia para crear e implementar estándares de red, dispositivos y esquemas de internetworking.
- Separa la compleja operación de una red en elementos más simples.

- Permite a los ingenieros centrarse en el diseño y desarrollo de funciones modulares ocupándose cada uno de su parte específica.

- Proporciona la posibilidad de definir interfaces estándar para compatibilidad "plug-and-play" e integración multifabricante.

1.2.1 Descripción de las siete capas

Capa de aplicación. Es la única capa que no presta servicio a otra puesto que es la capa de nivel superior del modelo OSI directamente relacionada con el usuario. La aplicación a través del software dialoga con los protocolos respectivos para acceder al medio. Por ejemplo, se accede a un procesador de textos por el servicio de transferencia de archivos de esta capa. Algunos protocolos relacionados con esta capa son: HTTP, correo electrónico, telnet.

Capa de presentación. Los datos formateados se proveen de diversas funciones de conversión y codificación que se aplican a los datos provenientes de la capa de aplicación. Estas funciones aseguran que estos datos enviados desde la capa de aplicación de un sistema origen podrán ser leídos por la capa de aplicación de otro sistema destino. Un ejemplo de funciones de codificación sería el cifrado de datos una vez que éstos salen de una aplicación. Por ejemplo, los formatos de imágenes jpeg y gif que se muestran en páginas web. Este formato asegura que todos los navegadores web puedan mostrar las imágenes, con independencia del sistema operativo utilizado. Algunos protocolos relacionados con esta capa son: JPEG, MIDI, MPEG, QUICKTIME.

Capa de sesión. Es la responsable de establecer, administrar y concluir las sesiones de comunicaciones entre entidades de la capa de presentación. La comunicación en esta capa consiste en peticiones de servicios y respuestas entre aplicaciones ubicadas en diferentes dispositivos. Un ejemplo de este tipo de coordinación podría ser el que tiene lugar entre un servidor y un cliente de base de datos.

Capa de transporte. Es la encargada de la comunicación confiable entre host, control de flujo y de la corrección de errores entre otras cosas. Los datos son divididos en segmentos identificados con un encabezado con un número de puerto que identifica la aplicación de origen. En esta capa funcionan protocolos como UDP y TCP, siendo este último uno de los más utilizados debido a su estabilidad y confiabilidad.

Capa de red. En esta capa se lleva a cabo el direccionamiento lógico que tiene carácter jerárquico, se selecciona la mejor ruta hacia el destino mediante el uso de tablas de enrutamiento a través del uso de protocolos de enrutamiento o por direccionamiento estático. Protocolos de capa de red: IP, IPX, RIP, IGRP, Apple Talk.

Capa de enlace de datos. Proporciona las comunicaciones entre puestos de trabajo en una primera capa lógica, transforma los voltios en tramas y las tramas en voltios. El direccionamiento físico y la determinación de si deben subir un mensaje a la pila de protocolo ocurren en esta capa. Está dividida en dos subcapas, la LLC Logical Link Control y la subcapa MAC. Protocolos de capa 2: Ethernet, 802.2, 802.3, HDLC, Frame-Relay.

Capa física. Se encarga de los medios, conectores, especificaciones eléctricas, lumínicas y de la codificación. Los bits son transformados en pulsos eléctricos, en luz o en radiofrecuencia para ser enviados según sea el medio en que se propaguen.

7	**APLICACIÓN**		HTML, HTTP, telnet, FTP, TFTP...
6	**PRESENTACIÓN**		JPEG, MIDI, MPEG, ASCII, Quicktime...
5	**SESIÓN**		Control de diálogo
4	**TRANSPORTE**		Control de flujo, TCP, UDP...
3	**RED**		Enrutamiento, IP, IPX, RIP, IGRP, APPLE TALK...
2	**ENLACE DE DATOS**	**LLC**	Ethernet, 802.2, 802.3, HDLC, Frame-Relay...
		MAC	
1	**FÍSICA**		Bits, pulsos...

1.3 FUNCIONES DE LA CAPA FÍSICA

La capa física define el medio, el conector y el tipo de señalización. Se especifican los requisitos necesarios para la correcta transmisión de los datos. Se establecen las características eléctricas, mecánicas y funcionales para activar, mantener y desactivar la conexión física entre sistemas finales.

La capa física especifica también características tales como niveles de voltaje, tasas de transferencia de datos, distancias máximas de transmisión y conectores, cada medio de red posee a su vez su propio ancho de banda y unidad máxima de transmisión (MTU).

El medio físico y los conectores usados para conectar dispositivos al medio vienen definidos por estándares de la capa física.

1.3.1 Dispositivos de la capa física

La capa física comprende los medios (cobre, fibra, RF), los conectores, transceivers, repetidores y hubs. Ninguno de ellos manipula los datos transmitidos sino que solo se encargan de transportarlos y propagarlos por la red.

Los repetidores se encargan de retransmitir y de retemporizar los pulsos eléctricos cuando la extensión del cableado supera las medidas específicas.

Los hubs son repetidores multipuesto, también llamados concentradores. Al recibir una trama inundan todos sus puertos obligando a todos los dispositivos conectados a cada uno de sus puertos a leer dichas tramas. Los transceivers son adaptadores de un medio a otro.

1.3.2 Estándares de la capa física

Los estándares de cableado se identifican siguiendo los siguientes conceptos:

10 Base T

Donde:

- **10** hace referencia a la velocidad de transmisión en Mbps (mega-bits por segundo), en este caso 10 Mbps.

- **Base** es la tecnología de transmisión (banda base, analógica o digital), en este caso digital.

- T se refiere al medio físico, en este caso par trenzado.

El siguiente cuadro muestra las características de los estándares más comunes:

Estándar	Medio físico	Distancia máxima	Comentarios
10Base 2	Cable coaxial fino de 50 ohms thinnet	185 metros	Conectores BNC
10Base 5	Cable coaxial grueso de 50 ohms Thinknet	500 metros	Conectores BNC
10Base FB	Fibra óptica	2000 metros	Cableado de backbone
100Base FX	Fibra óptica multimodo de 62,5/125 micrones	400 metros	Conectores ST, SC
100Base FX	Fibra óptica monomodo	10000 metros	Cableado de backbone
1000Base SX	Fibra óptica multimodo	260 metros	Varias señales a la vez
100Base LX	Fibra óptica monomodo de 9 micrones	3000 a 10000 metros	Cableado de backbone
10Base T	UTP categoría 3, 4, 5	100 metros	Conectores RJ-45
100Base T	UTP categoría 5	100 metros	Conectores RJ-45
100Base TX	UTP, STP categoría 6, 7	100 metros	Conectores RJ-45
1000Base T	UTP categoría 5, 6	100 metros	Conectores RJ-45 categoria 6

1.3.3 Medios de la capa física

La normativa EIE/TIA 568 fue creada en 1991 y establece los estándares de cableado estructurado, ampliada posteriormente a **568-A** y **568-B**.

Pin	Par	Función	Color
1	3	Transmite +	Blanco/verde
2	3	Transmite -	Verde
3	2	Recibe +	Blanco/ naranja
4	1	Telefonía	Azul
5	1	Telefonía	Blanco/ azul
6	2	Recibe -	Naranja
7	4	Respaldo	Blanco/marrón
8	4	Respaldo	Marrón

Orden de los pines correspondiente a la norma 568-A sobre un conector RJ-45

Pin	Par	Función	Color
1	3	Transmite +	Blanco/ naranja
2	3	Transmite -	Naranja
3	2	Recibe +	Blanco/ verde
4	1	Telefonía	Azul
5	1	Telefonía	Blanco/ azul
6	2	Recibe -	Verde
7	4	Respaldo	Blanco/marrón
8	4	Respaldo	Marrón

Orden de los pines correspondiente a la norma 568-B sobre un conector RJ-45

Cable directo: el orden de los pines es igual en ambos conectores, se debe utilizar la misma norma en cada extremo.

Extremo 1	Extremo 2
Blanco/naranja	Blanco/naranja
Naranja	Naranja
Blanco/verde	Blanco/verde
Azul	Azul
Blanco/azul	Blanco/azul
Verde	Verde
Blanco/marrón	Blanco/marrón
Marrón	Marrón

Cable directo 568 B

Extremo 1	Extremo 2
Blanco/verde	Blanco/verde
Verde	Verde
Blanco/naranja	Blanco/naranja
Azul	Azul
Blanco/azul	Blanco/azul
Naranja	Naranja
Blanco/marrón	Blanco/marrón
Marrón	Marrón

Cable directo 568 A

Cable cruzado: el orden de los pines varía en ambos extremos, se cruzan el 1-2 con el 3-6 y el 3-6 con el 1-2. El cable cruzado también es llamado **crossover**. Se utiliza para conectar dispositivos como, por ejemplo, PC-PC, PC-Router, Router-Router, etc.

Extremo 1	Extremo 2
Blanco/naranja	Blanco/verde
Naranja	Verde
Blanco/verde	Blanco/naranja
Azul	Azul
Blanco/azul	Blanco/azul
Verde	Naranja
Blanco/marrón	Blanco/marrón
Marrón	Marrón

Orden de los colores en ambos extremos de un cable cruzado

Cable consola: el orden de los pines es completamente inverso, 1-2-3-4-5-6-7-8 con el 8-7-6-5-4-3-2-1, respectivamente. El cable de consola también es llamado **rollover**.

1	al	**8**
2	al	**7**
3	al	**6**
4	al	**5**
5	al	**4**
6	al	**3**
7	al	**2**
8	al	**1**

Conector RJ-45

Cable UTP

Cable blincado STP

Fibra óptica

NOTA:

El enfoque principal de este libro está asociado con los estándares e implementaciones Ethernet e IEE 802.3.

1.3.4 Medios inalámbricos

Los medios inalámbricos transportan señales electromagnéticas mediante frecuencias de microondas y radiofrecuencias que representan los dígitos binarios de las comunicaciones de datos. Como medio en sí mismo, el sistema inalámbrico no se limita a condiciones físicas, como en el caso de los medios de fibra o de cobre. Sin embargo, el medio inalámbrico es susceptible a la interferencia y puede distorsionarse por dispositivos comunes como teléfonos inalámbricos domésticos, algunos tipos de luces fluorescentes, hornos microondas y otras comunicaciones inalámbricas.

Los estándares IEEE sobre las comunicaciones inalámbricas abarcan las capas física y de enlace de datos. Los cuatro estándares comunes de comunicación de datos que se aplican a los medios inalámbricos son:

- **IEEE estándar 802.11**: comúnmente denominada Wi-Fi, se trata de una tecnología LAN inalámbrica (red de área local inalámbrica,

WLAN) que utiliza una contención o sistema no determinista con un proceso de acceso a los medios de Acceso múltiple con detección de portadora/Prevención de colisiones (CSMA/CA).

- **IEEE estándar 802.15**: estándar de red de área personal inalámbrica (WPAN), comúnmente denominada Bluetooth, utiliza un proceso de emparejamiento de dispositivos para comunicarse a través de una distancia de 1 a 100 metros.

- **IEEE estándar 802.16**: comúnmente conocida como WiMAX (Interoperabilidad mundial para el acceso por microondas), utiliza una topología punto a multipunto para proporcionar un acceso de ancho de banda inalámbrico.

- **Sistema global para comunicaciones móviles** (GSM): incluye las especificaciones de la capa física que habilitan la implementación del protocolo Servicio general de radio por paquetes (GPRS) de capa 2 para proporcionar la transferencia de datos a través de redes de telefonía celular móvil.

1.4 FUNCIONES DE LA CAPA DE ENLACE DE DATOS

La finalidad de esta capa es proporcionar comunicación entre puestos de trabajo en una primera capa lógica que hay por encima de los bits del cable. El direccionamiento físico de los puestos finales se realiza en la capa de enlace de datos con el fin de facilitar a los dispositivos de red la determinación de si deben subir un mensaje a la pila de protocolo.

La capa de enlace de datos da soporte a servicios basados en la conectividad y no basados en ella, y proporciona la secuencia y control de flujo (no confundir con la capa de transporte). Tiene conocimiento de la topología a la que está afectada y donde se desempeña la tarjeta de red (**NIC**).

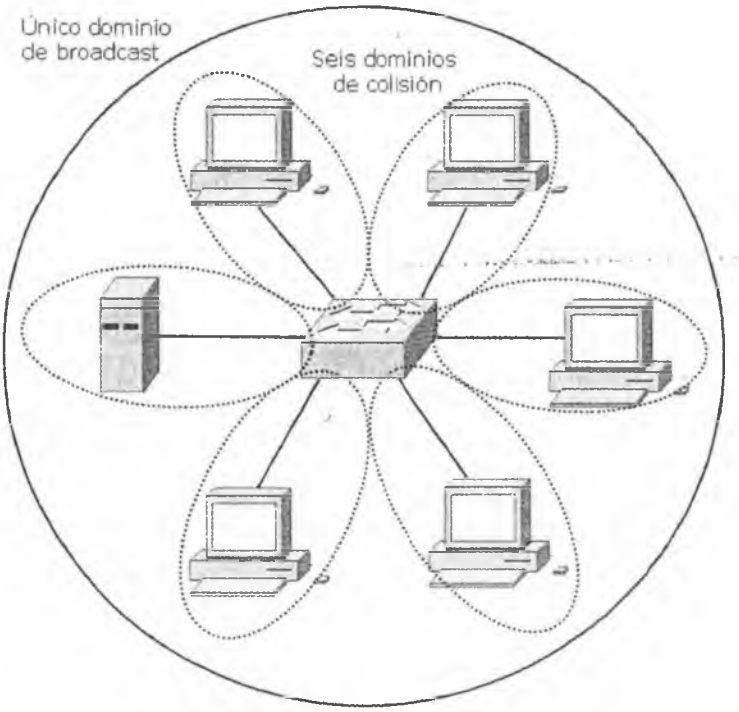
Está dividida en dos subcapas, la **LLC** (Logical Link Control 802.2), responsable de la identificación lógica de los distintos tipos de protocolos y el encapsulado posterior de los mismos para ser transmitidos a través de la red, y la subcapa **MAC** (802.3), responsable del acceso al medio, el direccionamiento físico, topología de la red, disciplina de la línea, notificación de errores, distribución ordenada de tramas y control óptimo de flujo. Las direcciones físicas de origen destino son representadas como direcciones de capa MAC.

1.4.1 Dispositivos de capa de enlace de datos

En la capa de enlace de datos se diferencian perfectamente los Dominios de Colisión y los Dominios de Difusión (ver más adelante). Los puentes y los switches dividen a la red en segmentos, estos a su vez crean dominios de colisión. Una colisión producida en un segmento conectado a un switch no afectará a los demás segmentos conectados al mismo switch. Sin embargo, los dispositivos de capa 2 no crean dominios de broadcast o difusión.

NOTA:

Un switch de 12 puertos utilizados tendrá 12 dominios de colisión y uno de difusión.



Los dispositivos de capa dos crean dominios de colisión pero mantienen un único Dominio de Broadcast.
Una colisión producida en un segmento NO afecta al resto

En un switch, el reenvío de tramas se controla por medio de hardware (ASIC). Esta tecnología permite que las funciones de conmutación puedan llevarse a cabo a una velocidad mucho mayor que por software. Debido a la tecnología **ASIC**, los switches proporcionan escalabilidad a velocidades de gigabits con una latencia baja. Los puentes funcionan a nivel de software por lo que poseen mayor latencia comparados con un switch.

Un dispositivo de capa 2 almacena en una memoria de contenido direccionable (CAM) las direcciones físicas de los dispositivos asociados a un segmento de red conectado directamente a un puerto determinado. De esta manera identificará inmediatamente por qué puerto enviar la trama. Si el dispositivo de destino está en el mismo segmento que el origen, el switch bloquea el paso de la trama a otro segmento. Este proceso se conoce como filtrado. Si el dispositivo de destino se encuentra en un segmento diferente, el switch envía la trama únicamente al segmento apropiado, técnica conocida como conmutación de capa dos. Si la dirección de destino es desconocida para el switch, o si se tratara de un broadcast, éste enviará la trama a todos los segmentos excepto a aquel de donde se ha recibido la información. Este proceso se denomina inundación.

La **NIC** o tarjeta de red opera en la capa de enlace de datos, no debe confundirse con la capa física a pesar de estar directamente conectada al medio ya que sus principales funciones radican en la capa 2. La NIC almacena en su propia ROM la dirección **MAC** que consta de 48 bits y viene expresada en 12 dígitos hexadecimales. Los primeros 24 bits, o 6 dígitos hexadecimales, de la dirección MAC contienen un código de identificación del fabricante o vendedor **OUI** (*Organizationally Unique Identifier*). Los últimos 24 bits, o 6 dígitos hexadecimales, están administrados por cada fabricante y presentan, por lo general, el número de serie de la tarjeta. La dirección de la capa de enlace de datos no tiene jerarquías, es decir, que es un direccionamiento plano.

Ejemplo de una dirección MAC o dirección física

00-11-85-F2-32-E5

Donde:

- **00-11-85** representa el código del fabricante.
- **F2-32-E5** representa el número de serie.

NOTA:

Para verificar el correcto funcionamiento de la tarjeta de red se realiza un ping a la dirección IP de la misma.

1.4.2 Características de las redes conmutadas

- Cada segmento genera su propio dominio de colisión.
- Todos los dispositivos conectados al mismo bridge o switch forman parte del mismo dominio de difusión.
- Todos los segmentos deben utilizar la misma implementación al nivel de la capa de enlace de datos como, por ejemplo, Ethernet o Token Ring.
- Si un puesto final concreto necesita comunicarse con otro puesto final a través de un medio diferente, se hace necesaria la presencia de algún dispositivo, como puede ser un router o un bridge de traducción, que haga posible el diálogo entre los diferentes tipos de medios.
- En un entorno conmutado, puede haber un dispositivo por segmento, y todos los dispositivos pueden enviar tramas al mismo tiempo, permitiendo de este modo que se comparta la ruta primaria.

1.5 FUNCIONES DE LA CAPA DE RED

La capa de red define cómo transportar el tráfico de datos entre dispositivos que no están conectados localmente en el mismo dominio de difusión, es decir, que pertenecen a diferentes redes. Para conseguir esta comunicación se necesita conocer las direcciones lógicas asociadas a cada puesto de origen y de destino y una ruta bien definida a través de la red para alcanzar el destino deseado. La capa de red es independiente de la de enlace de datos y, por tanto, puede ser utilizada para conectividad de medios físicos diferentes.

Las direcciones de capa 3, o direcciones lógicas, son direcciones jerárquicas. Esta jerarquía define primero las redes y luego a los dispositivos (nodos) pertenecientes a esas redes. Un ejemplo para la comprensión de una dirección jerárquica sería un número telefónico, donde primero se define el código del país, luego el estado y luego el número del usuario. Un esquema plano se puede

ejemplificar con un número de carné de identidad donde cada número es único y personal.

Una dirección lógica cuenta con dos partes bien definidas, una que identifica de forma única a la red dentro de un conjunto en la internetwork y la otra parte que representa al host dentro de estas redes. Con la suma o combinación de ambas partes se obtiene un identificador único para cada dispositivo. El router identifica dentro de la dirección lógica la porción perteneciente a la red con el fin de identificar la red donde enviar los paquetes.

NOTA:

Existen muchos protocolos de red, todos cumplen las mismas funciones de identificar redes y hosts. TCP/IP es el protocolo común más usado.

1.5.1 Direcciones de capa tres

Una dirección IPv4 se caracteriza por lo siguiente:

- Una dirección de 32 bits, dividida en cuatro octetos. Este direccionamiento identifica una porción perteneciente a la red y otra al host.
- A cada dirección IP le corresponde una máscara de red de 32 bits dividida en cuatro octetos. El router determina las porciones de red y host por medio de la máscara de red.
- Las direcciones IP generalmente se representan en forma decimal para hacerlas más comprensibles. Esta forma se conoce como decimal punteado o notación decimal de punto.

Dirección IP 172.16.1.3

Máscara 255.255.0.0

172	16	1	3
10101100	00010000	00000001	00000011
255	255	0	0
11111111	11111111	00000000	00000000
Porción de red		Porción de host	

Formato de una dirección IPv4

Las direcciones IPv6 miden 128 bits y son identificadores de interfaces individuales y conjuntos de interfaces. Más adelante se describe IPv6 con más detalle. Las direcciones IPv6 se asignan a interfaces, no a nodos. Como cada interfaz pertenece a un solo nodo, cualquiera de las direcciones unicast asignada a las interfaces del nodo se pueden usar como identificadores del nodo. Las direcciones IPv6 se escriben en hexadecimal, separadas por dos puntos. Los campos IPv6 tienen una longitud de 16 bits.

Ejemplo de una dirección IPv6:

24ae:0000:f2f3:0000:0000:0687:a2ff:6184

1.5.2 Comparación entre IPv4 e IPv6

Cuando se adoptó TCP/IP en los años ochenta, la versión 4 del IP (IPv4) ofrecía una estrategia de direccionamiento que, aunque resultó escalable durante algún tiempo, produjo una asignación poco eficiente de las direcciones.

A mediados de los años noventa se comenzaron a detectar las siguientes dificultades sobre IPv4:

- Agotamiento de las restantes direcciones de red IPv4 no asignadas. En ese entonces, el espacio de Clase B estaba a punto de agotarse.

- Se produjo un gran y rápido aumento en el tamaño de las tablas de enrutamiento de Internet a medida que las redes Clase C se conectaban en línea. La inundación resultante de nueva información en la red amenazaba la capacidad de los routers de Internet para ejercer una efectiva administración.

Durante las últimas dos décadas, se desarrollaron numerosas extensiones al IPv4. Estas extensiones se diseñaron específicamente para mejorar la eficiencia con la cual es posible utilizar un espacio de direccionamiento de 32 bits como **VLSM** y **CIDR** (ver más adelante).

Mientras tanto, se ha definido y desarrollado una versión más extensible y escalable del IP, la versión 6 del IP (IPv6). IPv6 utiliza 128 bits en lugar de los 32 bits que en la actualidad utiliza el IPv4. IPv6 utiliza números hexadecimales para representar los 128 bits. IPv6 proporciona 640 sextillones de direcciones. Esta versión del IP proporciona un número de direcciones suficientes para futuras necesidades de comunicación.

NOTA:

El direccionamiento IPv6 también es conocido como IPng o "IP de nueva generación".

1.5.3 Operación AND

Los routers determinan la ruta de destino a partir de la dirección de RED, estos comparan las direcciones IP con sus respectivas máscaras efectuando la operación booleana **AND**. Los routers ignoran el rango de host para encontrar la red destino a la que éste pertenece.

La operación AND consiste en comparar bit a bit la dirección IP y la máscara utilizando el siguiente razonamiento:

1 x 1 = 1

1 x 0 = 0

0 x 1 = 0

0 x 0 = 0

Dirección de host	**10101100.00100000.00000001.00000011**
Máscara de red	**11111111.11111111.00000000.00000000**
Dirección de red	**10101100.00100000.00000000.00000000**

En decimales:

Dirección de host	**172.**	**16.**	**1.**	**3**
Máscara de red	**255.**	**255.**	**0.**	**0**
Dirección de red	**172.**	**16.**	**0.**	**0**

1.5.4 Dispositivos de la capa de red

Los **routers** funcionan en la capa de red del modelo OSI separando los segmentos en dominios de colisión y difusión únicos. Estos segmentos están identificados por una dirección de red que permitirá alcanzar las estaciones finales. Los routers cumplen dos funciones básicas que son la de enrutar y conmutar los paquetes. Para ejecutar estas funciones registran en tablas de enrutamiento los datos necesarios para esta función.

Además de identificar redes y proporcionar conectividad, los routers deben proporcionar estas otras funciones:

- Los routers no envían difusiones de capa 2 ni tramas de multidifusión.
- Los routers intentan determinar la ruta más óptima a través de una red enrutada basándose en algoritmos de enrutamiento.
- Los routers separan las tramas de capa 2 y envían paquetes basados en direcciones de destino capa 3.
- Los routers asignan una dirección lógica de capa 3 individual a cada dispositivo de red; por tanto, los routers pueden limitar o asegurar el tráfico de la red basándose en atributos identificables con cada paquete. Estas opciones, controladas por medio de listas de acceso, pueden ser aplicadas para incluir o descartar paquetes.
- Los routers pueden ser configurados para realizar funciones tanto de puenteado como de enrutamiento.

- Los routers proporcionan conectividad entre diferentes LAN virtuales (VLAN) en entornos conmutados.

- Los routers pueden ser usados para desplegar parámetros de calidad de servicio para tipos específicos de tráfico de red.

Los routers conocen los diferentes destinos manteniendo tablas de enrutamiento que contienen la siguiente información:

- **Dirección de red**. Representa redes conocidas por el router. La dirección de red es específica del protocolo. Si un router soporta varios protocolos, tendrá una tabla por cada uno de ellos.

- **Interfaz**. Se refiere a la interfaz usada por el router para llegar a una red dada. Esta es la interfaz que será usada para enviar los paquetes destinados a la red que figura en la lista.

- **Métrica**. Se refiere al coste o distancia para llegar a la red de destino. Se trata de un valor que facilita al router la elección de la mejor ruta para alcanzar una red dada. Esta métrica cambia en función de la forma en que el router elige las rutas. Entre las métricas más habituales figuran el número de redes que han de ser cruzadas para llegar al destino (conocido también como saltos), el tiempo que se tarda en atravesar todas las interfaces hasta una red dada (conocido también como retraso), o un valor asociado con la velocidad de un enlace (conocido también como ancho de banda).

En la siguiente salida del router se observa una tabla de enrutamiento con las direcciones IP de destino (172.25.25.6/32), la métrica ([120/2]) y la correspondiente interfaz de salida Serial0.1.

```
Router2#show ip route rip
R    172.21.0.0/16 [120/1] via 172.25.2.1, 00:00:01, Serial0.1
R    172.22.0.0/16 [120/1] via 172.25.2.1, 00:00:01, Serial0.1
     172.25.0.0/16 is variably subnetted, 6 subnets, 3 masks
R    172.25.25.6/32 [120/2] via 172.25.2.1, 00:00:01, Serial0.1
R    172.25.25.1/32 [120/1] via 172.25.2.1, 00:00:01, Serial0.1
R    172.25.1.0/24 [120/1] via 172.25.2.1, 00:00:01, Serial0.1
R    172.25.0.0/16 [120/1] via 172.25.2.1, 00:00:01, Serial0.1
```

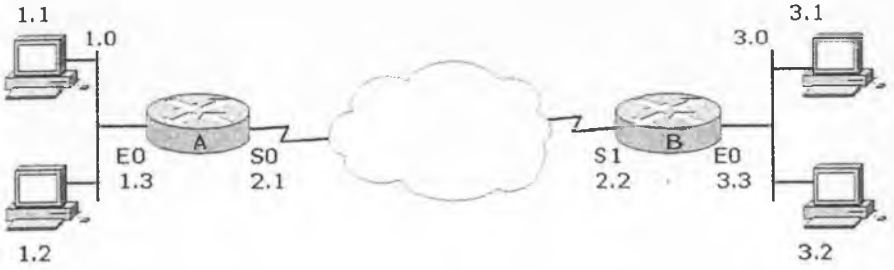
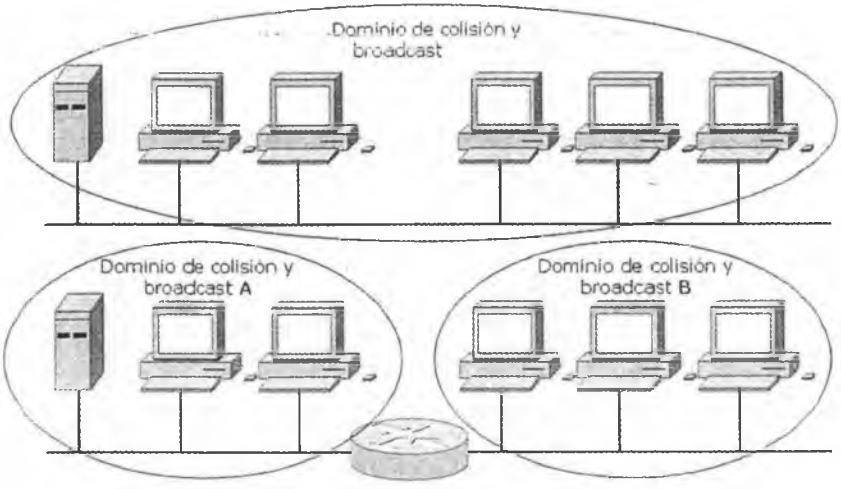


Tabla de enrutamiento Router A		
Red	Interfaz	Métrica
1	E0	0
2	S0	0
3	S0	1

Tabla de enrutamiento Router B		
Red	Interfaz	Métrica
1	S1	1
2	S1	0
3	E0	0

Además de las ventajas que aporta su uso en un campus, los routers pueden utilizarse también para conectar ubicaciones remotas con la oficina principal por medio de servicios WAN. Los routers soportan una gran variedad de estándares de conectividad al nivel de la capa física, lo cual ofrece la posibilidad de construir WAN. Además, pueden proporcionar controles de acceso y seguridad, que son elementos necesarios cuando se conectan ubicaciones remotas.



Los routers comunican redes diferentes creando dominios de difusión y de colisión, los broadcast de un segmento no inundan a los demás ni las colisiones afectan al resto

1.6 FUNCIONES DE LA CAPA DE TRANSPORTE

Para conectar dos dispositivos remotos es necesario establecer una conexión. La capa de transporte establece las reglas para esta interconexión. Permite que las estaciones finales ensamblen y reensamblen múltiples segmentos del mismo flujo de datos. Esto se hace por medio de identificadores que en **TCP/IP** reciben el nombre de números de puerto. La capa cuatro permite además que las aplicaciones soliciten transporte fiable entre los sistemas. Asegura que los segmentos distribuidos serán confirmados al remitente. Proporciona la retransmisión de cualquier segmento que no sea confirmado. Coloca de nuevo los segmentos en su orden correcto en el receptor. Proporciona control de flujo regulando el tráfico de datos.

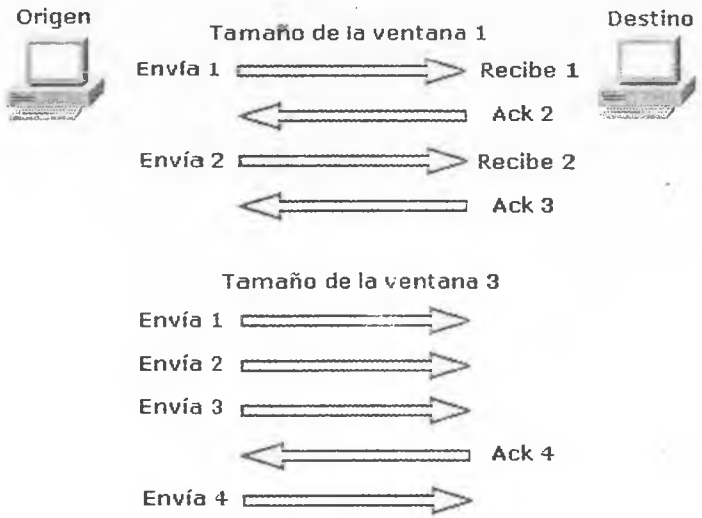
En la capa de transporte, los datos pueden ser transmitidos de forma fiable o no fiable. Para IP, el protocolo **TCP** (Protocolo de control de transporte) es fiable u orientado a conexión con un saludo previo de tres vías, mientras que **UDP** (Protocolo de datagrama de usuario) no es fiable, o no orientado a la conexión donde solo se establece un saludo de dos vías antes de enviar los datos.

1 al 1023	Puertos bien conocidos
1 al 255	Puertos públicos
256 al 1023	Asignados a empresas
Mayores al 1023	Definidos por el usuario

Números de puerto utilizados por TCP y UDP para identificar sesiones de diferentes aplicaciones

Un ejemplo de protocolo **orientado a conexión** puede compararse con una llamada telefónica, donde el interlocutor establece una conexión (marcando el número), verifica que el destinatario sea la persona que se espera (saludando recíprocamente) y finalmente estableciendo la conversación (envío de datos). El caso de un protocolo **no orientado a conexión** puede ser un envío postal, donde se envía la correspondencia sin establecer ningún aviso previo, ni acuse de recibo.

TCP utiliza una técnica llamada **ventanas**, donde se establece la cantidad de envío de paquetes antes de transmitir; mientras que en el **windowing** o de **ventana deslizante**, el flujo de envío de datos es negociado dinámicamente entre el emisor y el receptor. En las ventanas deslizantes o windowing cada acuse de recibo (ACK) confirma la recepción y el envío siguiente.



RECUERDE:

TCP, protocolo confiable de capa de transporte orientado a conexión
UDP, protocolo **NO** confiable de capa de transporte **NO** orientado a conexión
Un protocolo orientado a conexión es el que previamente establece un saludo antes de enviar los datos, como es el ejemplo de una llamada telefónica, donde se establece un saludo de tres vías. Un protocolo No orientado a conexión es el que no establece saludo previo antes de enviar los datos como es el caso de un envío postal donde se establece un saludo de dos vías

Nº	Modelo OSI	Funciones	Protocolos
7	APLICACIÓN	Nivel usuario, software, aplicaciones	HTTP, Telnet, SNMP,
6	PRESENTACIÓN	Representación y traducción de datos, formateo, cifrado	JPG, MP3, DOC
5	SESIÓN	Reglas, separar datos de las aplicaciones, establece sesiones entre aplicaciones	NFS, Linux
4	TRANSPORTE	Comunicación confiable, corrección de errores, control de flujo, establece, mantiene y finaliza comunicaciones	UDP,TCP
3	RED	Direccionamiento lógico, determinación de ruta	IP, IPX, RIP, ARP, ICMP
2	ENLACE DE DATOS	Direccionamiento físico, mapa topológico, acceso al medio	Ethernet, PPP, HDLC
1	FÍSICA	Codificación, transmisión	EIE/TIA 568

1.7 ETHERNET

Ethernet es la tecnología de acceso al medio más popular, es escalable, económica y fácilmente integrable a nuevas aplicaciones, se pueden obtener arquitecturas de LAN a velocidades de Gigabit sobre cobre y la resolución de fallos suele ser simple y rápida. Ethernet opera sobre la capa de enlace de datos y física del modelo OSI. Sin embargo, no es determinista ni ofrece jerarquías.

Ethernet es una tecnología conflictiva de máximo esfuerzo, todos los equipos de trabajo que se conectan al mismo medio físico reciben las señales enviadas por otros dispositivos. Si dos estaciones transmiten a la vez, se genera una colisión. Si no existieran mecanismos que detectasen y corrigiesen los errores de estas colisiones, Ethernet no podría funcionar.

Ethernet fue creada en colaboración por Intel, Digital y Xerox, originalmente se implementó como Ethernet 802.3, half-duplex, limitada al transporte de datos por solo un par de cobre a la vez (recibe por un par y transmite por otro pero no al mismo tiempo). Posteriormente la tecnología Ethernet full-duplex permitió recibir y enviar datos al mismo tiempo libre de colisiones. El uso más adecuado del ancho de banda permite casi duplicarse al poder transmitir y recibir al 100% de capacidad. Sin embargo, esta tecnología no es tan económica y es solo aplicable a dispositivos que lo permitan.

En el diseño de una red Ethernet se debe tener especial cuidado con los llamados **dominios de colisión** y **dominios de difusión** (broadcast) debido a que la excesiva cantidad de colisiones o de broadcast (tormentas de broadcast) harían inaceptable el funcionamiento de Ethernet.

1.7.1 Dominio de colisión

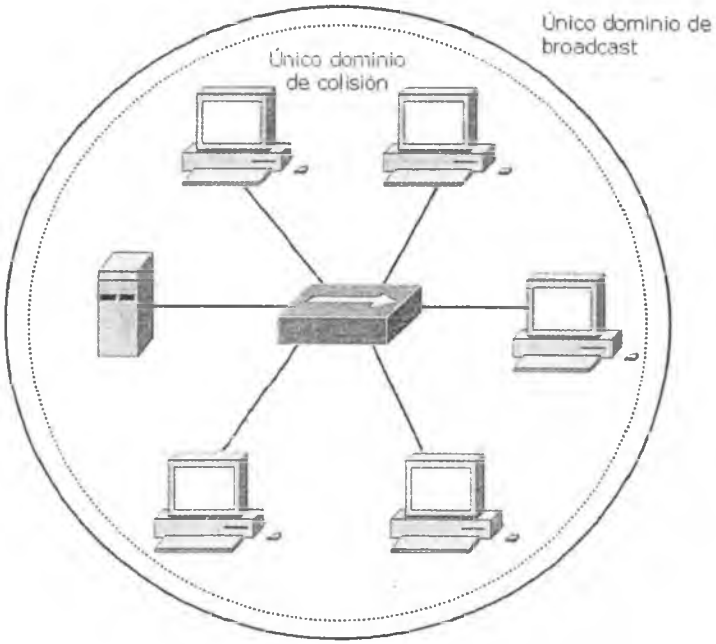
- Grupo de dispositivos conectados al mismo medio físico, de tal manera que si dos dispositivos acceden al medio al mismo tiempo, el resultado será una colisión entre las dos señales. Como resultado de estas colisiones se produce un consumo inadecuado de recursos y de ancho de banda. Cuanto menor sea la cantidad de dispositivos afectados a un dominio de colisión mejor desempeño de la red.

1.7.2 Dominio de difusión

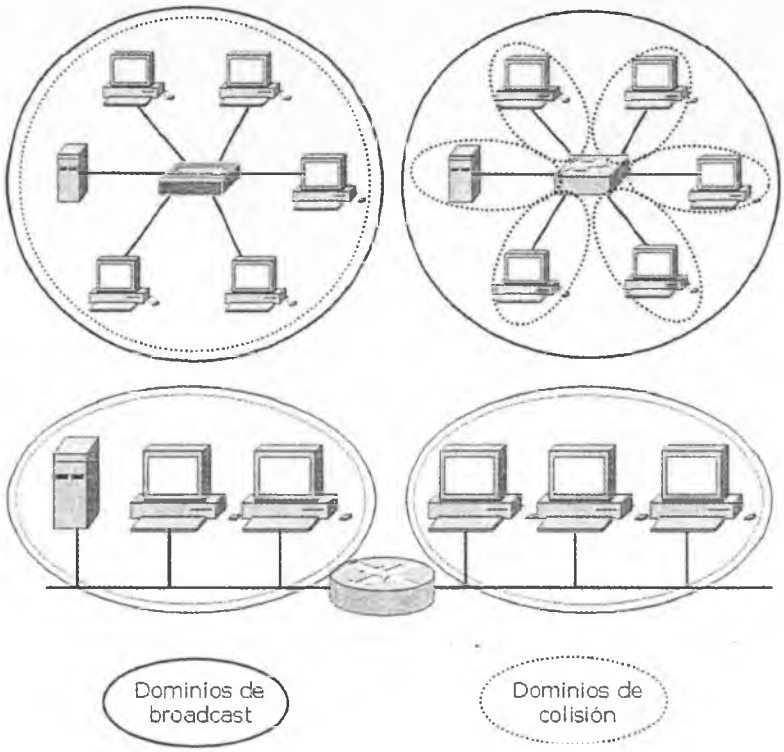
Grupo de dispositivos de la red que envían y reciben mensajes de difusión entre ellos. Una cantidad excesiva de estos mensajes de difusión (broadcast) provocará un bajo rendimiento en la red, una cantidad exagerada (tormenta de

broadcast) dará como resultado el mal funcionamiento de la red hasta tal punto de poder dejarla completamente congestionada.

Los hubs o concentradores tienen un único dominio de colisión, eso quiere decir que si dos equipos provocan una colisión en un segmento asociado a un puerto del hub, todos los demás dispositivos aun estando en diferentes puertos se verán afectados. De igual manera se verían afectados si una estación envía un broadcast, debido a que un hub también tiene un solo dominio de difusión.



Los dispositivos conectados a través de un hub comparten el mismo dominio de colisión y de broadcast. Las colisiones en el medio afectarán por igual a todos los hosts del segmento



Comparativa entre dominios de colisión y dominios de difusión en dispositivos de tres capas diferentes

NOTA:

Asócie a los routers como los dispositivos que crean dominios de difusión y a los switches como los que crean dominios de colisión.

1.7.3 CSMA/CD

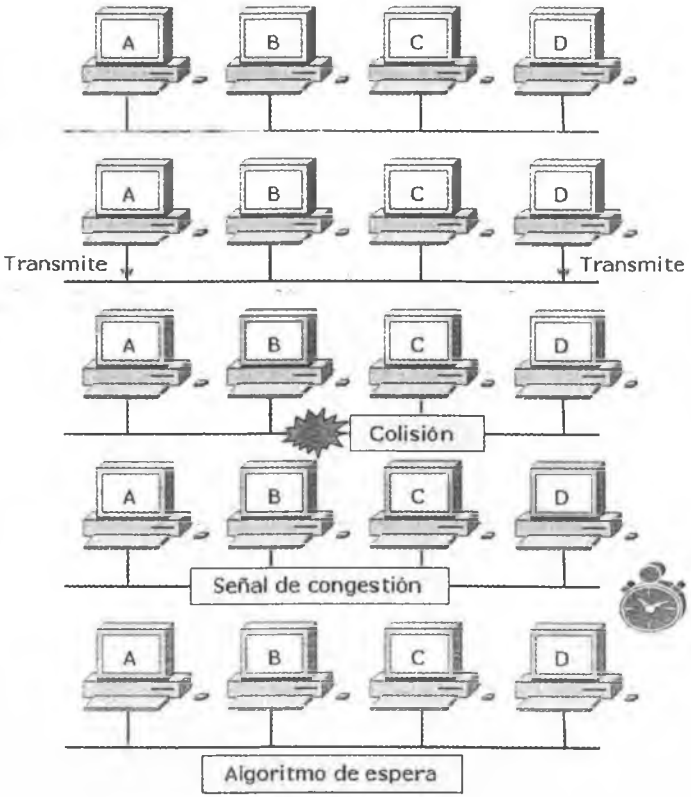
La tecnología Ethernet utiliza para controlar las colisiones dentro de un determinado segmento el protocolo **CSMA/CD** (acceso múltiple con detección de portadora y detección de colisiones). En la práctica, esto significa que varios puestos pueden tener acceso al medio y que, para que un puesto pueda acceder a dicho medio, deberá detectar la portadora para asegurarse de que ningún otro puesto esté utilizándolo. Si el medio se encuentra en uso, el puesto procederá a mantener en suspenso el envío de datos. En caso de que haya dos puestos que no

detectan ningún otro tráfico, ambos tratarán de transmitir al mismo tiempo, dando como resultado una colisión.

A partir de esta colisión las estaciones emiten una señal de congestión para asegurarse de que existe una colisión y se genera un algoritmo de espera con el que las estaciones retransmitirán aleatoriamente.

NOTA:

El ejemplo más claro de CSMA/CD es el de "escucho y luego transmito".



Secuencia de una colisión en un entorno Ethernet

1.7.4 Formato básico de una trama Ethernet

El formato de la trama del estándar **IEEE 802.3** y el de Ethernet creado por Xerox son muy similares y compatibles, solo difieren en algunas pequeñas cuestiones de concepto. IEEE 802.3 se basa en las especificaciones recogidas por los estándares del Instituto de Ingenieros Eléctricos y Electrónicos, a partir de Ethernet mientras que Ethernet II es una versión actualizada de Ethernet.

Longitud máxima: **1518** Bytes
Longitud mínima: **64** Bytes

- **Preámbulo**. Secuencia de valores alternados 1 y 0 usados para la sincronización y para detectar la presencia de señal, indica el inicio de la trama.

- **Dirección de destino**. Este campo identifica la dirección MAC del dispositivo que debe recibir la trama. La dirección de destino puede especificar una dirección individual o una dirección multicast destinada a un grupo de estaciones. Una dirección destino con todos los bits en 1 se refiere a todos los dispositivos de la red denominada dirección de broadcast o difusión.

- **Dirección de origen**. Este campo identifica la dirección MAC del dispositivo que debe enviar la trama.

- **Tipo**. Indica el tipo de protocolo de capa superior.

- **Datos**. Este campo contiene los datos transferidos desde el origen hasta el destino. El tamaño máximo de este campo es de 1500 bytes. Si el tamaño de este campo es menor de 46 bytes, entonces es necesario el uso del campo siguiente (Pad) para añadir bytes hasta que el tamaño de la trama alcance el valor mínimo.

- **FSC**. Campo de comprobación de la trama, este campo contiene un valor de chequeo de redundancia de 4 bytes (CRC) para verificación de errores. La estación origen efectúa un cálculo y lo transmite como parte de la trama. Cuando la trama es recibida por el destino, este realiza un chequeo idéntico. Si el valor calculado no coincide con el valor en el campo, el destino asume que ha sido un error durante la transmisión y entonces descarta la trama completa.

Los estándares originales Ethernet definen el tamaño mínimo de trama como 64 bytes y el máximo como 1518 bytes. Estas cantidades incluyen todos los bytes de la trama menos los comprendidos en el preámbulo. En 1998 se promovió una iniciativa con el fin de incrementar el tamaño máximo del campo de datos de 1500 a 9000 bytes. Las tramas más largas (tramas gigantes) proveen un uso más eficiente del ancho de banda en la red a la vez que reducen la cantidad de tramas a procesar.

1.7.5 Proceso de encapsulación de los datos

El proceso desde que los datos son incorporados al ordenador hasta que se transmiten al medio se llama encapsulación. Estos datos son formateados, segmentados, identificados con el direccionamiento lógico y físico para finalmente ser enviados al medio. A cada capa del modelo OSI le corresponde una **PDU** (Unidad de Datos) siguiendo por lo tanto el siguiente orden de encapsulamiento:

1. **Datos**
2. **Segmentos**
3. **Paquetes**
4. **Tramas**
5. **Bits**

APLICACIÓN	**DATOS**
PRESENTACIÓN	
SESIÓN	
TRANSPORTE	**SEGMENTOS**
RED	**PAQUETES**
ENLACE DE DATOS	**TRAMAS**
FÍSICA	**BITS**

Relación entre capas del modelo OSI y su correspondiente PDU

Debido a que posiblemente la cantidad de los datos sea demasiada, la capa de transporte desde el origen se encarga de segmentarlos para así ser empaquetados debidamente, esta misma capa en el destino se encargará de reensamblar los datos y colocarlos en forma secuencial, ya que no siempre llegan a su destino en el orden en que han sido segmentados, así mismo acorde al protocolo que se esté utilizando habrá o no corrección de errores. Estos segmentos son empaquetados (paquetes o datagramas) e identificados en la capa de red con la dirección lógica o IP correspondiente al origen y destino. Ocurre lo mismo con la dirección MAC en la capa de enlace de datos formándose las tramas o frames para ser transmitidos a través de alguna interfaz. Finalmente las tramas son enviadas al medio desde la capa física.

NOTA:

El proceso inverso se realiza en el desino y se llama desencapsulación de datos.

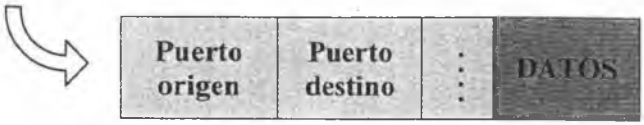
Secuencia de la encapsulación de datos:

Se crean los datos a través de una aplicación

Datos

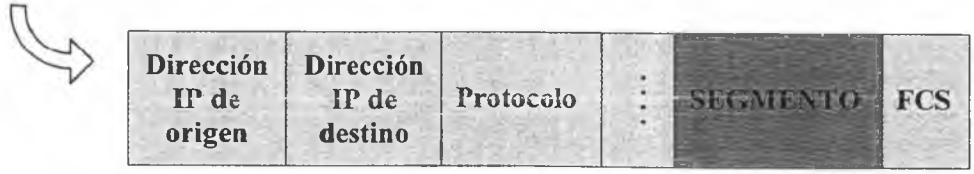
Los datos son segmentados

Segmentos



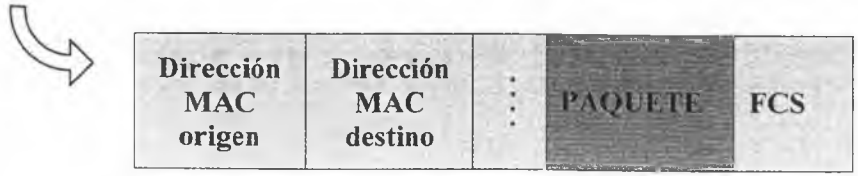
Se coloca el encabezado IP

Paquetes



Se agrega el encabezado MAC

Tramas



Se envía al medio

Bits

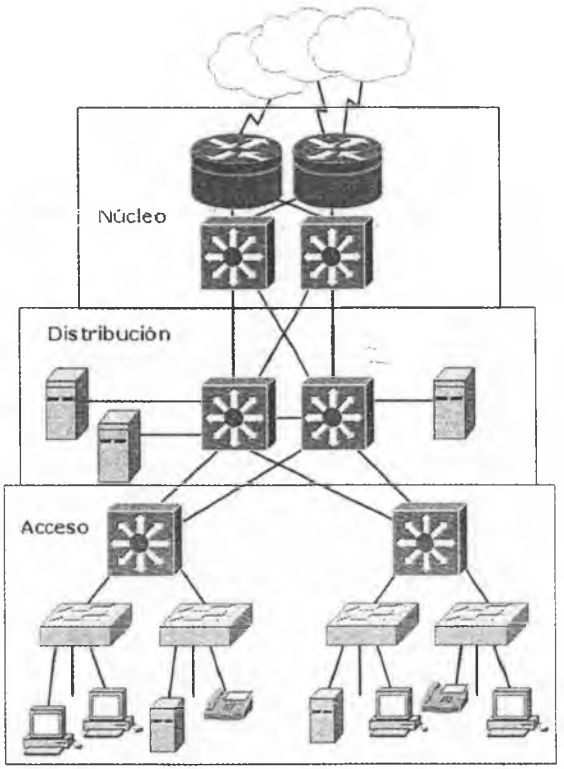
10010111010011110010101000111101010000.....

1.8 MODELO JERÁRQUICO DE TRES CAPAS

Con el fin de simplificar el diseño, implementación y administración de las redes, Cisco utiliza un modelo jerárquico para describir la red. Aunque la práctica de este método suele estar asociada con el proceso de diseño de una red, es importante comprender el modelo para poder determinar el equipo y características que van a necesitar en la red. Un modelo jerárquico acelera la convergencia, mantiene posibles problemas aislados por capas y reduce la sobrecarga en los dispositivos.

El modelo se compone de tres capas:

- Capa de acceso.
- Capa de distribución.
- Capa de núcleo.



Modelo jerárquico de tres capas

1.8.1 Capa de acceso

La capa de acceso de la red es el punto en el que cada usuario se conecta a la red. Esta es la razón por la cual la capa de acceso se denomina a veces capa de puesto de trabajo, capa de escritorio o de usuario. Los usuarios así como los recursos a los que estos necesitan acceder con más frecuencia están disponibles a nivel local. El tráfico hacia y desde recursos locales está confinado entre los recursos, switches y usuarios finales.

En la capa de acceso podemos encontrar múltiples grupos de usuarios con sus correspondientes recursos. En muchas redes no es posible proporcionar a los usuarios un acceso local a todos los servicios, como archivos de bases de datos, almacenamiento centralizado o acceso telefónico a la Web. En estos casos, el tráfico de usuarios que demandan estos servicios se desvía a la siguiente capa del modelo: la capa de distribución.

Algunas de las funciones de la capa de acceso son:

- Interconexión de los diferentes grupos de trabajo hacia la capa de distribución.
- Segmentación en múltiples dominios de colisión.
- Brinda soporte a tecnologías como Ethernet y Wireless.
- Implementación de redes virtuales (VLAN).

1.8.2 Capa de distribución

La capa de distribución marca el punto medio entre la capa de acceso y los servicios principales de la red. La función primordial de esta capa es realizar funciones tales como enrutamiento, filtrado y acceso a WAN.

En un entorno de campus, la capa de distribución abarca una gran diversidad de funciones, entre las que figuran las siguientes:

- Servir como punto de concentración para acceder a los dispositivos de capa de acceso.
- Enrutar el tráfico para proporcionar acceso a los departamentos o grupos de trabajo y entre las diferentes VLAN.
- Segmentar la red en múltiples dominios de difusión/multidifusión.

- Traducir los diálogos entre diferentes tipos de medios, como Token Ring y Ethernet.

- Proporcionar servicios de seguridad y filtrado.

La capa de distribución puede resumirse como la capa que proporciona una conectividad basada en una determinada política, dado que determina cuándo y cómo los paquetes pueden acceder a los servicios principales de la red. La capa de distribución determina la forma más rápida para que la petición de un usuario (como un acceso al servidor de archivos) pueda ser remitida al servidor. Una vez que la capa de distribución ha elegido la ruta, envía la petición a la capa de núcleo. La capa de núcleo podrá entonces transportar la petición al servicio apropiado.

1.8.3 Capa de núcleo

La capa del núcleo, principal o core se encarga de desviar el tráfico lo más rápidamente posible hacia los servicios apropiados. Normalmente, el tráfico transportado se dirige o proviene de servicios comunes a todos los usuarios. Estos servicios se conocen como servicios globales o corporativos. Algunos de ellos pueden ser e-mail, el acceso a Internet o videoconferencia.

Cuando un usuario necesita acceder a un servicio corporativo, la petición se procesa al nivel de la capa de distribución. El dispositivo de la capa de distribución envía la petición del usuario al núcleo. Este se limita a proporcionar un transporte rápido hasta el servicio corporativo solicitado. El dispositivo de la capa de distribución se encarga de proporcionar un acceso controlado a la capa de núcleo.

Para la capa de núcleo se deben tomar en cuenta los siguientes conceptos:

- Esta capa debe ser diseñada para una alta velocidad de transferencia y mínima latencia.

- No se debe dar soporte a grupos de trabajo ni enrutamiento entre VLAN.

- El tráfico debe haber sido filtrado en la capa anterior.

- Los protocolos de enrutamientos utilizados deben ser de rápida convergencia y redundantes.

RECUERDE:

Capa	Funciones	Dispositivos
Núcleo	Conmuta el tráfico hacia el servicio solicitado, comunicación rápida y segura	**Routers, switch multicapa**
Distribución	Enrutamiento, filtrado, acceso WAN, seguridad basada en políticas, servicios empresariales, enrutamiento entre VLANS, definición de dominios de broadcast y multicast	**Router**
Acceso	Define Dominios de colisión. estaciones finales, ubicación de usuarios, servicios de grupos de trabajos, VLANS	**Hub, switch**

1.9 MODELO TCP/IP

El Departamento de Defensa de EE.UU. (DoD) creó el modelo de referencia **TCP/IP** porque necesitaba una red que pudiera sobrevivir ante cualquier circunstancia. Para tener una mejor idea, imagine un mundo, cruzado por numerosos tendidos de cables, alambres, microondas, fibras ópticas y enlaces satelitales. Entonces, imagine la necesidad de transmitir datos independientemente del estado de un nodo o red en particular. El DoD requería una transmisión de datos confiable hacia cualquier destino de la red, en cualquier circunstancia. La creación del modelo TCP/IP ayudó a solucionar este difícil problema de diseño. Desde entonces, TCP/IP se ha convertido en el estándar en el que se basa Internet. Al leer sobre las capas del modelo TCP/IP, tenga en cuenta el diseño original de Internet. Recordar su propósito ayudará a reducir las confusiones.

El modelo TCP/IP tiene cuatro capas: la capa de aplicación, la capa de transporte, la capa de Internet y la capa de acceso de red. Es importante observar que algunas de las capas del modelo TCP/IP poseen el mismo nombre que las capas del modelo OSI. Resulta fundamental no confundir las funciones de las capas

de los dos modelos ya que estas se desempeñan de diferente manera en cada modelo.

OSI	TCP/IP	Protocolos
APLICACIÓN PRESENTACIÓN SESIÓN	APLICACIÓN	Telnet, FTP, LPD, SNMP,TFTP, SMTP, NFS, HTTP, X Windows
TRANSPORTE	TRANSPORTE	TCP, UDP
RED	INTERNET	ICMP, BOOTP, ARP, RARP, IP
ENLACE DE DATOS FÍSICA	RED	Ethernet, Fast-Ethernet, Token Ring, FDDI

Comparativa entre el modelo OSI y el modelo TCP/IP

1.9.1 Protocolos de la capa de aplicación

Los protocolos describen el conjunto de normas y convenciones que rigen la forma en que los dispositivos de una red intercambian información. Algunos de los protocolos de la capa de Aplicación del modelo TCP/IP son:

- **Telnet**. Protocolo de emulación de terminal estándar que se usa para la conexión de terminales remotas, permitiendo que los usuarios se registren en dichos sistemas y utilicen los recursos como si estuvieran conectados localmente.

- **FTP**. Protocolo utilizado para transferir archivos entre host de red de manera confiable ya que utiliza un mecanismo orientado a conexión.

- **TFTP**. Versión simplificada de FTP que permite la transferencia de archivos de un host a otro a través de una red de manera menos confiable.

- **DNS**. El sistema de denominación de dominio es utilizado en Internet para convertir los nombres de los nodos de red en direcciones.

- **SMTP**. Protocolo simple de transferencia de correo basado en texto utilizado para el intercambio de mensajes de correo electrónico entre distintos dispositivos. Se basa en el modelo cliente-servidor, donde un cliente envía un mensaje a uno o varios receptores.

- **SNMP**. Protocolo de administración de redes utilizado casi con exclusividad en redes TCP/IP. El SNMP brinda una forma de monitorizar y controlar los dispositivos de red y de administrar configuraciones, recolección de estadísticas, desempeño y seguridad.

- **DHCP**. Protocolo de configuración dinámica del host. Protocolo que proporciona un mecanismo para asignar direcciones IP de forma dinámica, de modo que las direcciones se pueden reutilizar automáticamente cuando los hosts ya no las necesitan.

1.9.2 Protocolos de la capa de transporte

Los protocolos de la capa de transporte se encargan de dar soporte a la capa superior brindando apoyo enviando los datos sin importar el contenido de los mismos. Los dos protocolos extensamente conocidos para tal proceso son:

- **TCP**. Protocolo de control de transmisión, es básicamente el más utilizado, tiene control de flujo, reensamblado de paquetes y acuses de recibo. Es un protocolo orientado a conexión muy seguro que utiliza un saludo de tres vías antes del envío de los datos. En párrafos anteriores se hace una descripción más en detalle del funcionamiento de TCP.

- **UDP**. El protocolo de datagrama del usuario es en general menos seguro que TCP, no tiene corrección de errores y es del tipo no orientado a conexión, los datos se envían sin verificar previamente el destino. A pesar de ello es muy utilizado por el bajo consumo de recursos de red.

1.9.3 Números de puertos

Los números de puerto son utilizados por TCP y UDP para identificar sesiones de diferentes aplicaciones, a continuación se detallan los más comunes:

Número de puerto	Protocolo
7	Echo
9	Discard
13	Daytime
19	Character Generator
20	FTP Data Connections
21	File Transfer Protocol
23	Telnet
25	Simple Mail Transport Protocol
37	Time
53	Domain Name Service
43	Nickname
49	TAC Access Control System
69	Trivial File Transfer Protocol
70	Gopher
79	Finger
80	World Wide Web

101	NIC hostname server
109	Post Office Protocol v2
110	Post Office Protocol v3
111	Sun Remote Procedure Call
113	Ident Protocol
119	Network News Transport Protocol
179	Border Gateway Protocol

1.9.4 Protocolos de la capa de Internet

Estos son algunos de los protocolos más usados que operan en la capa de Internet del modelo TCP/IP:

- **IP**. Protocolo de Internet, proporciona un enrutamiento de paquetes no orientado a conexión de máximo esfuerzo. IP no se ve afectado por el contenido de los paquetes, sino que busca una ruta hacia el destino.

- **ARP**. Protocolo de resolución de direcciones, determina la dirección de la capa de enlace de datos, la dirección MAC, para las direcciones IP conocidas.

- **RARP**. Protocolo de resolución inversa de direcciones, determina las direcciones IP cuando se conoce la dirección MAC.

- **ICMP**. Protocolo de mensajes de control en Internet, suministra capacidades de control y envío de mensajes. Herramientas tales como PING y tracert utilizan ICMP para poder funcionar, enviando un paquete a la dirección destino específica y esperando una determinada respuesta.

NOTA:

La capa de Internet también es llamada capa de Interred o capa de red.

RECUERDE:

1 al 1023	Puertos bien conocidos
1 al 255	Puertos públicos
256 al 1023	Asignados a empresas
Mayores al 1023	Definidos por el usuario

1.10 CASO PRÁCTICO

1.10.1 Prueba de conectividad TCP/IP

Imagine que desea comprobar la conectividad de un host, usted enviará un ping a la dirección IP del host en cuestión esperando algún tipo de respuesta o mensaje de error (protocolo ICMP).

El host emisor debe conocer las direcciones físicas y lógicas del destino. Antes de enviar el ping buscará en su tabla ARP la dirección MAC del destinatario. Si este no supiera cuál es la dirección física de aquel, enviará una petición ARP con la dirección IP del receptor y la MAC en forma de broadcast. El receptor responderá con su MAC haciendo posible que el emisor agregue a su tabla esa dirección y envíe por fin el PING. Si el host destino está dentro de otra red, quien responde en este caso es el router entregando su propia MAC para recibir el paquete y conmutarlo a la red correspondiente, es lo que se llama **ARP Proxy**.

Desde su PC abra una ventana de línea de comandos, ejecute **ipconfig** para verificar su configuración. Ejecute **arp –a** para ver el contenido de la tabla ARP.

Lance un **ping** al host de destino y vuelva a ejecutar **arp –a**. Verifique las diferencias entre la tabla anterior y la actual.

1.11 MATEMÁTICAS DE REDES

1.11.1 Números binarios

Los dispositivos emiten y reciben pulsos eléctricos o luminosos. Estos pulsos poseen dos estados, SÍ y NO. Este sistema de dos signos se le llama binario. Matemáticamente hablando un sistema binario está compuesto por dos estados de unos y ceros siendo, por tanto, una potencia en base 2. En informática se llama bits a la unidad que tiene también dos estados; un byte es un grupo de ocho bits.

Un octeto o un byte se expresa de la siguiente manera:

00000000

Cada uno de estos bits que componen el octeto posee dos estados, 1 y 0, obteniendo, por tanto, 256 estados con todas las combinaciones posibles.

00000000
00000001
00000010
00000011
00000100
.....
01111111
11111111

Para que estos bits sean más entendibles conviene trasladarlos al modo decimal al que se está más acostumbrado cotidianamente, por tanto, si son potencias de 2, su valor será:

$2^7\ 2^6\ 2^5\ 2^4\ 2^3\ 2^2\ 2^1\ 2^0$
$2^0 = 1$
$2^1 = 2$
$2^2 = 4$
$2^3 = 8$
$2^4 = 16$
$2^5 = 32$
$2^6 = 64$
$2^7 = 128$

Los bits que resulten iguales a 1 tendrán el valor correspondiente a esa potencia, mientras que los que permanezcan en 0 tendrán un valor igual a cero, finalmente se suma el conjunto de los decimales resultantes y se obtiene el equivalente en decimal.

1.11.2 Conversión de binario a decimal

Para pasar de binario a decimal es posible utilizar la siguiente técnica:

0000001 (en binario) = 0000002^0 (en decimal) =1

En el octeto: 0+0+0+0+0+0+0+1

01001001 (en binario) = $02^5002^3002^0$(en decimal) = 73

En el octeto: 0+64+0+0+8+0+0+1

Dígito binario	octavo	séptimo	sexto	quinto	cuarto	tercero	segundo	primero
Potencia de dos	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Valor decimal	128	64	32	16	8	4	2	1

1.11.3 Conversión de decimal a binario

Para pasar de decimal a binario es posible utilizar la siguiente técnica:

Convertir a binario el número decimal 195:

Valor binario	**Acción**	**Resta**	**Resultado**
128	¿Entra en **195**?	195-128	**Sí** = 67
64	¿Entra en **67**?	67-64	**Sí** = 3
32	¿Entra en **3**?	3-32	**No**, siguiente
16	¿Entra en **3**?	3-16	**No**, siguiente
8	¿Entra en **3**?	3-8	**No**, siguiente
4	¿Entra en **3**?	3-4	**No**, siguiente
2	¿Entra en **3**?	3-2	**Sí** = 1
1	¿Entra en **1**?	1-1	**Sí** = 0

Donde los **SÍ** equivalen al valor binario **UNO** y los **NO** al valor binario **CERO.**

Por lo tanto, 195 es equivalente en binario a 11000011

1.11.4 Números hexadecimales

Los números hexadecimales se basan en potencias de 16, utilizando símbolos alfanuméricos, la siguiente tabla le ayudará a convertir números hexadecimales en binarios o en decimales:

Número decimal	Número hexadecimal	Número binario
0	0	0000
1	1	0001
2	2.	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

1.11.5 Conversión de números hexadecimales

Siguiendo el ejemplo anterior, el número **195** es igual al número binario:

11000011

Divida este octeto en dos grupos de cuatro: **1100 0011**

Busque el valor correspondiente en la tabla de estos dos grupos de bits.

Al número binario **1100** le corresponde el número hexadecimal **C**.

Al número binario **0011** le corresponde el número hexadecimal **3**.

Por lo tanto, **195** es igual a **11000011** en binario y al **C3** en hexadecimal. Para que no existan confusiones los números hexadecimales se identifican con un **0x** delante, en este caso **0xC3**.

El proceso inverso será, por ejemplo, el número hexadecimal **0xAE** donde:

A es igual a **1010**

E es igual a **1110**

Por lo tanto, **0xAE** es igual el número binario **10101110** si se convierte este número a decimal:

$$2^7+0+2^5+0+2^3+2^2+2^1+0 = \underline{174}$$

NOTA:

Existen varias técnicas para hacer conversiones de un sistema numérico a otro; un matemático, un físico o un informático podrían utilizar diferentes métodos de conversión con iguales resultados. El estudiante podrá utilizar el método que crea más conveniente según su propio criterio.

1.12 DIRECCIONAMIENTO IPv4

Para que dos dispositivos se comuniquen entre sí, es necesario poder identificarlos claramente. Una dirección IPv4 es una secuencia de unos y ceros de 32 bits. Para hacer más comprensible el direccionamiento, una dirección IP aparece escrita en forma de cuatro números decimales separados por puntos. La notación decimal punteada es un método más sencillo de comprender que el método binario de unos y ceros.

Esta notación decimal punteada también evita que se produzca una gran cantidad de errores por transposición, que sí se produciría si solo se utilizaran números binarios. El uso de decimales separados por puntos permite una mejor comprensión de los patrones numéricos.

Una dirección IPv4 consta de dos partes definidas por la llamada máscara de red. La máscara puede describirse a través de una notación decimal punteada o con el prefijo /X, donde X es igual a la cantidad de bitd en 1 que contine dicha máscara. Una parte identifica la red donde se conecta el sistema y la segunda identifica el sistema en particular de esa red. Este tipo de dirección recibe el nombre de dirección jerárquica porque contiene diferentes niveles. Una dirección IPv4 combina estos dos identificadores en un solo número. Este número debe ser exclusivo, porque las direcciones repetidas harían imposible el enrutamiento. La primera parte identifica la dirección de la red del sistema. La segunda parte, la del host, identifica qué máquina en particular de la red.

Dirección IP 172.16.1.3

Máscara 255.255.0.0 o /16

172	16	1	3
10101100	00010000	00000001	00000011
255	255	0	0
11111111	11111111	00000000	00000000
Porción de red		Porción de host	

Ejemplo de una dirección IPv4

1.12.1 Tipos de direcciones IPv4

Dentro del rango de direcciones de cada red IPv4, existen tres tipos de direcciones:

- **Dirección de red**: la dirección en la que se hace referencia a la red. Dentro del rango de dirección IPv4 de una red, la dirección más baja se reserva para la dirección de red. Esta dirección tiene un 0 para cada bit de host en la porción de host de la dirección

- **Dirección de broadcast**: una dirección especial que se utiliza para enviar datos a todos los hosts de la red.

- **Direcciones host**: las direcciones asignadas a los dispositivos finales de la red.

1.12.2 Tipos de comunicación IPv4

En una red IPv4, los hosts pueden comunicarse de tres maneras diferentes:

- **Unicast**: el proceso por el cual se envía un paquete de un host a un host individual.

- **Broadcast**: el proceso por el cual se envía un paquete de un host a todos los hosts de la red.

- **Multicast**: el proceso por el cual se envía un paquete de un host a un grupo seleccionado de hosts.

Estos tres tipos de comunicación se usan con diferentes objetivos en las redes de datos. En los tres casos, se coloca la dirección IPv4 del host de origen en el encabezado del paquete como la dirección de origen.

1.12.3 Tráfico unicast

La comunicación unicast se usa para una comunicación normal de host a host, tanto en una red de cliente/servidor como en una red punto a punto. Los paquetes unicast utilizan la dirección host del dispositivo de destino como la dirección de destino y pueden enrutarse a través de una internetwork. Sin embargo, los paquetes broadcast y multicast usan direcciones especiales como la dirección de destino. Al utilizar estas direcciones especiales, los broadcasts están generalmente restringidos a la red local.

1.12.4 Tráfico de broadcast

Existe un direccionamiento particular cuando los bits están todos en UNOS llamada dirección de **broadcast**, o de difusión. Este direccionamiento identifica al host origen, mientras que como destino tiene a todos los dispositivos que integran el mismo dominio. Una cantidad excesiva de estas difusiones provocará una tormenta de broadcast que hará ineficiente el uso de la red, consumiendo gran cantidad de ancho de banda y haciendo que los host utilicen demasiados recursos al estar "obligados" a leer esos paquetes ya que están dirigidos a todos los host que integran ese dominio de broadcast.

NOTA:

Para esta certificación, todas las comunicaciones entre dispositivos son comunicaciones unicast a menos que se indique lo contrario

1.12.5 Clases de direcciones IPv4

La RFC1700 agrupa rangos de direcciones unicast en tamaños específicos llamados direcciones de clase. Las direcciones IPv4 se dividen en clases para definir las redes de tamaño pequeño, mediano y grande. Las direcciones Clase A se asignan a las redes de mayor tamaño. Las direcciones Clase B se utilizan para las redes de tamaño medio y las de Clase C para redes pequeñas. Dentro de cada rango existen direcciones llamadas privadas para uso interno que no veremos en Internet. Las direcciones de clase D son de uso multicast y las de clase E, experimentales.

Direccionamiento **Clase A**:

Rango de direcciones IP: **1.0.0.0** a **127.0.0.0**
Máscara de red: **255.0.0.0** o **/8**

Direcciones privadas: **10.0.0.0** a **10.255.255.255**

Direccionamiento **Clase B**:

Rango de direcciones IP: **128.0.0.0** a **191.255.0.0**
Máscara de red: **255.255.0.0** o **/16**

Direcciones privadas: **172.16.0.0** a **172.31.255.255**

Direccionamiento **Clase C**:

Rango de direcciones IP: **192.0.0.0** a **223.255.255.0**
Máscara de red: **255.255.255.0** o **/24**

Direcciones privadas: **192.168.0.0** a **192.168.255.255**

Direccionamiento **Clase D**:

Rango de direcciones IP: **224.0.0.0** a **239.255.255.255**

Uso multicast o multidifusión

Direccionamiento **Clase E**:

Rango de direcciones IP: **240.0.0.0** a **254.255.255.255**

Uso experimental o científico

En números binarios:

Las clases A comienzan con 00xxxxxx
Las clases B comienzan con 10xxxxxx
Las clases C comienzan con 11xxxxxx
Las clases D comienzan con 111xxxxx
Las clases E comienzan con 1111xxxx

1.12.6 Direcciones IPv4 especiales

Hay determinadas direcciones que no pueden asignarse a los hosts por varios motivos. También hay direcciones especiales que pueden asignarse a los hosts pero con restricciones en la interacción de dichos hosts dentro de la red.

- **Direcciones de red y de broadcast**: no es posible asignar la primera ni la última dirección a los hosts dentro de cada red. Éstas son, respectivamente, la dirección de red y la dirección de broadcast del rango de host.

- **Ruta predeterminada**: la ruta predeterminada IPv4 se representa como 0.0.0.0. La ruta predeterminada se usa como ruta por defecto cuando no se dispone de una ruta más específica. El uso de esta dirección también reserva todas las direcciones en el bloque de direcciones 0.0.0.0 al 0.255.255.255 (0.0.0.0 /8).

- **Loopback**: es una de las direcciones reservadas IPv4. La dirección de loopback **127.0.0.1** es una dirección especial que los hosts utilizan para dirigir el tráfico hacia ellos mismos. La dirección de loopback crea un método de acceso directo para las aplicaciones y servicios TCP/IP que se ejecutan en el mismo dispositivo para comunicarse entre sí. Al utilizar la dirección de loopback en lugar de la dirección host IPv4 asignada, dos servicios en el mismo host pueden desviar las capas inferiores de la pila TCP/IP. También es posible hacer ping a la dirección de loopback para probar la configuración de TCP/IP en el host local.

- **Direcciones link-local**: las direcciones IPv4 del bloque de direcciones desde 169.254.0.0 hasta 169.254.255.255 (169.254.0.0 /16) se encuentran designadas como direcciones link-local. El sistema operativo puede asignar automáticamente estas direcciones al host local en entornos donde no se dispone de una configuración IP. Se puede usar en una red de punto a punto o para un host que no pudo obtener automáticamente una dirección de un servidor de protocolo de configuración dinámica de host (DHCP).

1.12.7 Subredes

Las redes IPv4 se pueden dividir en redes más pequeñas, para el mayor aprovechamiento de las mismas, que llamadas subredes, además de contar con esta flexibilidad, la división en subredes permite que el administrador de la red brinde contención de broadcast y seguridad de bajo nivel en la LAN. La división en subredes, además, ofrece seguridad ya que el acceso a las otras subredes está disponible solamente a través de los servicios de un router. Las clases de direcciones IP disponen de 256 a 16,8 millones de hosts según su clase.

El proceso de creación de subredes comienza pidiendo "prestado" al rango de host la cantidad de bits necesaria para la cantidad de subredes requeridas. Se debe tener especial cuidado en esta acción de pedir ya que deben quedar como mínimo dos bits del rango de host.

La máxima cantidad de bits disponibles para este propósito depende del tipo de clase:

- **Clase A**, cantidad disponible **22** bits.
- **Clase B**, cantidad disponible **14** bits. .
- **Clase C**, cantidad disponible **6** bits.

Cada bit que se toma del rango de host posee dos estados 0 y 1, por lo tanto, si se toman tres bit existirán 8 estados diferentes:

Bits prestados	Bits de host	Valor decimal
000	00000	0
001	00000	32
010	00000	64
011	00000	96
100	00000	128
101	00000	160
110	00000	192
111	00000	224

El número de subredes que se puede usar es igual a: 2 elevado a la potencia del número de bits asignados a subred.

$$2^N = \text{Número de subredes}$$

Donde N es la cantidad de bits tomados al rango de host.

Por lo tanto, si se quieren crear **5** subredes, es decir, cumpliendo la fórmula 2^N, tendrá que tomar del rango de host 3 bits:

$$2^3 = 8$$

Observe que no siempre el resultado es exacto, en este caso se pedían 5 subredes pero se obtendrán 8.

1.12.8 Procedimiento para la creación de subredes

Paso 1 - Piense en binarios.

Paso 2 - Encuentre la máscara adecuada para la cantidad de subredes que le solicitan, independientemente de la dirección IP, lo que nos importa es la cantidad de bits libres.

Razone, red clase C, el primer octeto, el segundo y el tercero corresponden a la dirección de red, por lo tanto, trabaje con el cuarto octeto correspondiente a los host. De izquierda a derecha tome la cantidad de bits necesarios de la máscara para la cantidad de subredes que le solicitan:

Crear 10 subredes a partir de una red Clase C

Según la formula 2^N debemos tomar 4 bits del rango de host, por lo tanto:

$$2^4 = 16$$

Recuerde que no siempre los valores son exactos

Máscara de red 255.255.255.0

Rango de red **Rango de host**

11111111.11111111.11111111.00000000

Cuarto octeto **00000000**

11110000

Coloque en **1** (uno) los bits que resultaron de la operación anterior y súmelos, recuerde el valor de cada bit dentro del octeto: 128, 64, 32, 16, 8, 4, 2, 1

Se obtiene:

11110000

128+64+32+16 = 240

La máscara de subred de clase C para obtener 10 subredes válidas es:

255.255.255.240

Paso 3 - Identifique las correspondientes direcciones IP de las subredes restando a 256, que es la cantidad máxima de combinaciones que tiene un octeto (0 a 255), el valor de la máscara obtenida. Este número será la dirección de la primera subred utilizable que a su vez es el incremento o la constante para determinar las siguientes subredes.

256-240 = 16

El resultado indica la primera dirección válida de subred, en este caso 16.

Número de subred	Valor del octeto	Valor decimal
1	00000000	0
2	00010000	16
3	00100000	32
4	00110000	48
5	01000000	64
6	01010000	80
7	01100000	96
8	01110000	112

9	**10000000**	**128**
10	**10010000**	**144**
11	**10100000**	**160**
12	**10110000**	**176**
13	**11000000**	**192**
14	**11010000**	**208**
15	**11100000**	**224**
16	**11110000**	**240**

El incremento constante en este caso será de 16

Paso 4 - Obtenga las direcciones IP de las subredes (observe el cuadro anterior).

Dirección IP de la red original: 192.168.1.0 255.255.255.0

Dirección IP de la 1ª subred: 192.168.1.0 255.255.255.240
Dirección IP de la 2ª subred: 192.168.1.16 255.255.255.240
Dirección IP de la 3ª subred: 192.168.1.32 255.255.255.240
Dirección IP de la 4ª subred: 192.168.1.48 255.255.255.240
.....

Dirección IP de la 13ª subred: 192.168.1.224 255.255.255.240
Dirección IP de la 14ª subred: 192.168.1.240 255.255.255.240

La máscara **255.255.255.255** se denomina **máscara de nodo** que identifica un host en particular.

Otra forma de identificar las máscaras es sumar los bits en uno y colocarlos detrás de la dirección IP separados por una barra:

Dirección IP de la red original: 192.168.1.0/24

Dirección IP de la 1ª subred: 192.168.1.0/28
Dirección IP de la 2ª subred: 192.168.1.16/28

Dirección IP de la 3ª subred: 192.168.1.32/28
Dirección IP de la 4ª subred: 192.168.1.48/28
.....

Dirección IP de la 13ª subred: 192.168.1.224/28
Dirección IP de la 14ª subred: 192.168.1.240/28

Paso 5 - Identifique el rango de host que integran las subredes.

Hasta ahora se ha trabajado con los bits del rango de red, es decir de izquierda a derecha en el octeto correspondiente, ahora lo haremos con los bits restantes del rango de host, es decir de derecha a izquierda.

Tomemos como ejemplo la subred 196.168.1.16/28 y apliquemos la fórmula 2^N-2, nos han quedado 4 bits libres, por lo tanto:

$$2^4-2=16-2=14$$

Estas subredes tendrán 14 host válidos utilizables en cada una.

Número de host	Valor del octeto	Valor decimal
	00010000	Subred
1	00010001	17
2	00010010	18
3	00010011	19
4	00010100	20
5	00010101	21
6	00010110	22
7	00010111	23
8	00011000	24

9	00011001	25
10	00011010	26
11	00011011	27
12	00011100	28
13	00011101	29
14	00011110	30
15	00011111	Broadcast

El rango de host válido para la subred 192.168.1.16/28 será:

192.168.1.17 al **192.168.1.30**

El mismo procedimiento se lleva a cabo con el resto de las subredes:

N° de subred	Rango de host válidos	Broadcast
192.168.1.0	1 al 14	15
192.168.1.16	17 al 30	31
192.168.1.32	31 al 62	63
192.168.1.64	65 al 78	79
192.168.1.80	81 al 94	95
192.168.1.96	97 al 110	111
.....	.....	.....
192.168.1.224	225 al 238	239
192.168.1.240	241 al 254	255

NOTA:

La dirección de broadcast de una subred será la inmediatamente inferior a la subred siguiente.

RECUERDE:

Paso 1

Piense en binarios.

Paso 2

Encuentre la máscara contando de izquierda a derecha los bits que tomará prestados del rango de host. Cada uno tendrá dos estados, un bit dos subredes, dos bits cuatro subredes, tres bits ocho subredes, etc.

Paso 3

Reste a 256 la suma de los bits que ha tomado en el paso anterior para obtener la primera subred válida que a su vez será el incremento.

Paso 4

Obtenga las direcciones IP de las subredes siguientes sumando a la primera subred el incremento para obtener la segunda, luego a la segunda más el incremento para obtener la tercera y así hasta la última.

Paso 5

Identifique el rango de host y la correspondiente dirección de broadcast de cada subred.

RECUERDE:

Clase A:

Red	Host			Máscara de red			
10	0	0	0	255	0	0	0

Clase B:

Red		Host		Máscara de red			
172	16	0	0	255	255	0	0

Clase C:

Red			Host	Máscara de red			
192	168	0	0	255	255	255	0

RECUERDE:

Las diferentes clases de redes se pueden identificar fácilmente en números binarios observando el comienzo del primer octeto, puesto que:

Las clases **A** comienzan con **00**xxxxxx

Las clases **B** comienzan con **10**xxxxxx

Las clases **C** comienzan con **11**xxxxxx

Las clases **D** comienzan con **111**xxxxx

Las clases **E** comienzan con **1111**xxxx

1.13 MÁSCARAS DE SUBRED DE LONGITUD VARIABLE

El crecimiento exponencial de las redes ha hecho que el direccionamiento IPv4 no permita un desarrollo y una escalabilidad acorde a lo deseado por los administradores de red. IPv4 pronto será reemplazado por IP versión 6 (IPv6) como protocolo dominante de Internet. IPv6 posee un espacio de direccionamiento prácticamente ilimitado y algunos administradores ya han empezado a implementarlo en sus redes. Para dar soporte al direccionamiento IPv4 se ha creado **VLSM** (máscara de subred de longitud variable) que permite incluir más de una máscara de subred dentro de una misma dirección de red. VLSM es soportado únicamente por protocolos sin clase tales como OSPF, RIPv2 y EIGRP.

El uso de las máscaras de subred de longitud variable permite el uso más eficaz del direccionamiento IP. Al permitir niveles de jerarquía se pueden resumir diferentes direcciones en una sola, evitando gran cantidad de actualizaciones de ruta.

Hasta ahora las direcciones de host que pertenecían a la subred "cero" se perdían al no poder utilizarlos. Si se configura el comando **ip subnet-zero** todas las direcciones de host pertenecientes a esta subred se podrán admitir como válidas.

Observe el ejemplo:

La red 192.168.1.0/24 se divide en subredes utilizando una máscara de subred de 28 bits.

Hasta ahora la primer subred utilizable era la 192.168.1.16/28; configurando el router con el comando **ip subnet-zero** la dirección IP 192.168.1.0/28 será una dirección válida pudiendo sumar 14 host válidos más al direccionamiento total.

Siguiendo el esquema de direccionamiento anterior una de las subredes que surgen de la división se utilizará para un enlace serial entre dos routers. En este caso la máscara de 28 bits permite el uso válido de 14 host desperdiciándose 12 direcciones de host para este enlace. El uso de VLSM permite volver a dividir más subredes en otra subred, en este caso la máscara ideal sería una /30.

1.13.1 Proceso de creación de VLSM

Siguiendo el ejemplo anterior, la red 192.168.1.0/24 será dividida en 16 subredes válidas:

Se obtienen las siguientes subredes

192.168.1.0/28
192.168.1.16/28
192.168.1.32/28
192.168.1.48/28
192.168.1.64/28
192.168.1.80/28
192.168.1.96/28
192.168.1.112/28
192.168.1.128/28
192.168.1.144/28
192.168.1.160/28
192.168.1.176/28
192.168.1.192/28
192.168.1.208/28
192.168.1.224/28
192.168.1.240/28

Observe que se tomará en cuenta la 192.168.1.0 al configurar el comando ip subnet-zero

Para el enlace serial entre los routers se utilizará una máscara /30 que nos permita el uso de dos host. Elija una de las subredes creadas en el paso anterior, esta subred elegida NO podrá utilizarse con la máscara /28 puesto que se seguirá dividiendo en subredes más pequeñas.

Paso 1 - Piense en binario.

Paso 2 - La red 192.168.1.0/24 se divide en subredes con una máscara /28, escriba en binario el último octeto.

```
/24      /28
|0000|0000 =0
|0001|0000 =16
|0010|0000 =32
|....|.....
|1000|0000 =128
|....|.....
```

Paso 3 - Elija una de las subredes para dividirla con una máscara /30, en este caso la 128. Trace una línea que separe los bits con la máscara /28 y otra que separe los bits con máscara /30. Las subredes se obtienen haciendo las

combinaciones correspondientes entre el bit 128 y los contenidos entre las dos paralelas.

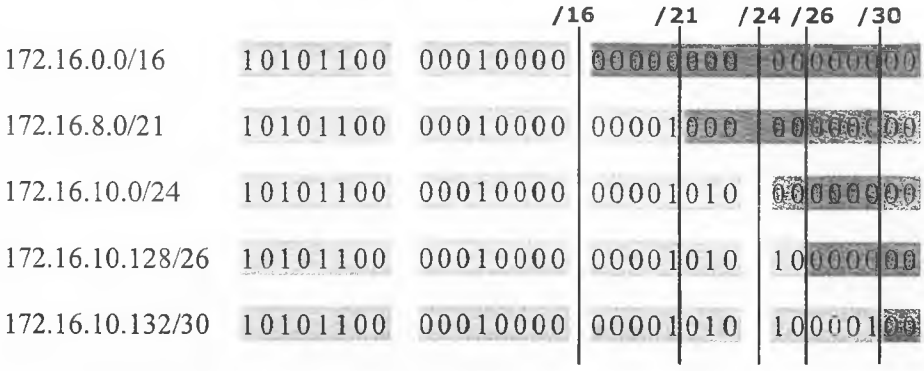
```
/24   /28 /30
|1000|00|00 =128
|1000|01|00 =132
|1000|10|00 =136
|1000|11|00 =140
```

Paso 4 - Las direcciones de host se obtienen haciendo la combinación con los dos bits libres en cada una de las subredes obtenidas.

Ejemplo con una red Clase B:

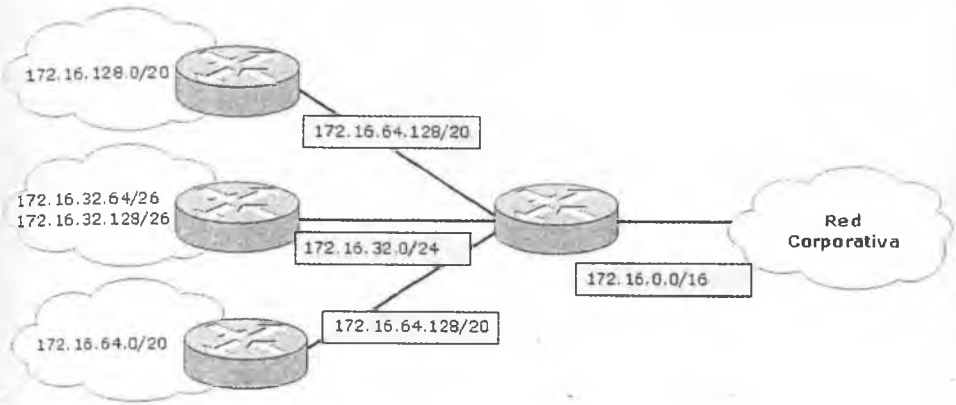
- **172.16.0.0/16** se divide en subredes con una máscara /21, para seguir el proceso elija la:
- **172.16.8.0/21** se divide en subredes con una máscara /24, para seguir el proceso elija la:
- **172.16.10.0/24** se divide en subredes con una máscara /26, para seguir el proceso elija la:
- **172.16.10.128/26** se divide en subredes con una máscara /30
- **172.16.10.132/30**

En binarios:



1.14 RESUMEN DE RUTA CON VLSM

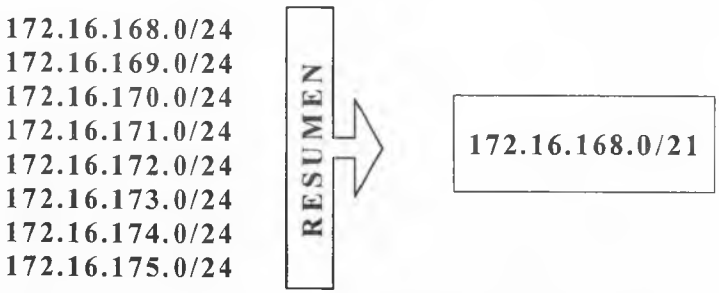
El resumen de ruta **CIDR** (agregación de ruta o supernetting) reduce la cantidad de rutas que un router debe mantener en sus tablas anunciando y manteniendo una sola dirección que contenga a las demás.



El router de resumen tiene múltiples entradas de redes consecutivas, siendo éste el principal factor en el resumen de ruta, pero solo anunciará al router remoto la red que contiene a todas las demás

1.14.1 Explicación de funcionamiento de CIDR

Imagine que un router posee un rango de redes directamente conectadas, de la 172.16.168.0/24 a la 172.16.175.0/24. El router buscará el bit común más alto para determinar cuál será el resumen de ruta con la máscara más pequeña posible.



En binarios:

Dirección de subred	Primer octeto	Segundo octeto	Tercer octeto		Cuarto octeto
172.16.168.0/24	10101100	00010000	10101	000	00000000
172.16.169.0/24	10101100	00010000	10101	001	00000000
172.16.170.0/24	10101100	00010000	10101	010	00000000
172.16.171.0/24	10101100	00010000	10101	011	00000000
172.16.172.0/24	10101100	00010000	10101	100	00000000
172.16.173.0/24	10101100	00010000	10101	101	00000000
172.16.174.0/24	10101100	00010000	10101	110	00000000
172.16.175.0/24	10101100	00010000	10101	111	00000000
	Bits comunes = 21 Resumen 172.16.168.0/21			Bits no comunes o de host	

Por lo tanto, para el rango especificado el router utilizará la dirección **172.16.168.0/21** para el resumen de ruta solicitado.

1.15 DIRECCIONAMIENTO IPv6

IPv6 ha estado en desarrollo desde mediados de los noventa y durante varios años. Se había anunciado al principio como el protocolo que podría expandir el direccionamiento IP, llevar *IP mobile* a la madurez y finalmente ser capaz de incorporar seguridad a nivel de capa 3. Esas afirmaciones son correctas pero hay que tener en cuenta que a nivel de capa 3 esas capacidades de IPv6 han sido aportadas a IPv4 en los pasados años. Actualmente las direcciones IPv4 son escasas y la mayor razón en Internet para evolucionar a IPv6 es la necesidad de un mayor direccionamiento.

Una de las razones de que el direccionamiento IPv4 sea demasiado escaso es que no ha sido asignado eficientemente. Las direcciones de clase A son excesivamente grandes para la mayoría de las organizaciones ya que soportan unas 16.777.214 direcciones de host, mientras que las direcciones de clase C soportan

solo 254 direcciones de host. Como resultado de esto muchas organizaciones hacen peticiones de clase B que soportan 65.534 direcciones de host, pero hacen solo un uso parcial de dicho rango.

Inicialmente un dispositivo IP requería una dirección pública. Para prevenir el agotamiento de las direcciones IPv4 la **IETF** (*Internet Engineering Task Force*) adoptó el uso de **CIDR** (*Classless Interdomain Routing*), **VLSM** (*Variable-Length Subnet Mask*) y **NAT** (*Network Address Translation*). CIDR y VLSM trabajan juntas a la hora de mejorar el direccionamiento, mientras que NAT oculta clientes y minimiza la necesidad de direcciones públicas. Otra de las razones de escasez de direcciones públicas es que no han sido asignadas equitativamente a lo largo del mundo. Una gran cantidad de direccionamiento es ocupada por EE.UU. mientras que Europa es el siguiente en la lista con una larga porción de direcciones. Asia, en cambio tiene un número insuficiente de direcciones en comparación con su población, aunque la percepción desde EE.UU. es que todavía existe espacio libre en el direccionamiento IPv4 en Asia, se reconoce la necesidad de implementar IPv6 y así obtener más direccionamiento.

Otra razón para considerar la necesidad de un mayor direccionamiento es el crecimiento exponencial de la población mundial con el persistente crecimiento de consumibles electrónicos que requieren el uso de direcciones IP.

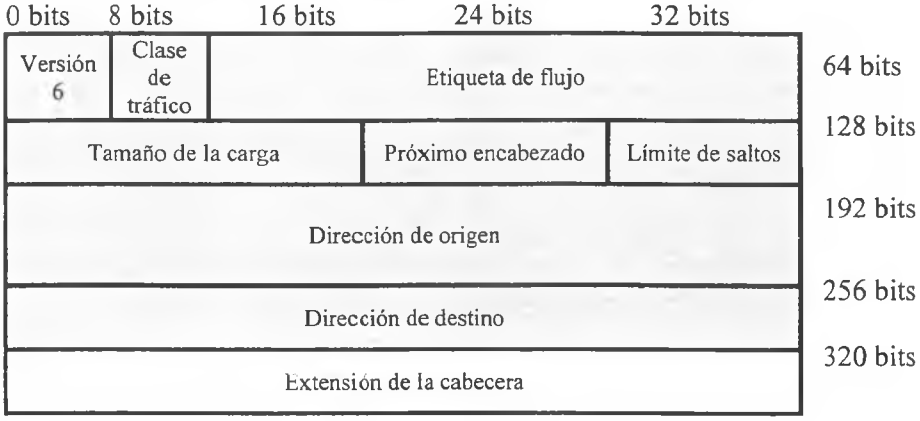
Esta necesidad de direccionamiento IP podría ser atenuada intentando utilizar NAT y asignaciones temporales a través de DHCP, pero teniendo sistemas intermedios manipulando los paquetes complican el diseño y la resolución de problemas. El concepto del diseño de Internet con innumerables sistemas intermedios no hace que NAT trabaje adecuadamente, sin embargo es un mal necesario.

La longitud de una dirección IPv6 es lo primero que sale a relucir, son 128 bits lo que hace $\mathbf{2^{128}}$ direcciones IPv6 disponibles. Varias de estas direcciones dan funciones especiales y están reservadas pero aun así quedarían disponibles aproximadamente $\mathbf{5x10^{28}}$ direcciones IP por cada habitante del planeta. Lo que permitiría que el direccionamiento pueda crecer sin preocupaciones en contraposición al direccionamiento IPv4 cuya cantidad está limitada a $\mathbf{2^{32}}$.

En IPv6 se utiliza una cabecera más simplificada que IPv4, haciendo que el procesamiento sea más eficiente, permitiendo un mecanismo más flexible y a su vez extensible a otras características. Una de esas características es la movilidad, *movile IP* es un estándar de la IETF que permite a los usuarios con dispositivos wireless estar conectados de manera transparente y moverse a cualquier sitio sin restricciones.

La cabecera IPv6 es optimizada para procesadores de 32 a 64 bits y las extensiones de cabecera permiten la expansión sin tener que forzar a que los campos que no se usan se estén transmitiendo constantemente.

Las principales diferencias entre las cabeceras de las dos versiones es la longitud de los campos de origen y destino. También hay otros campos que son aparentes como checksum, fragmentación y la etiqueta de flujo.



1.15.1 Formato del direccionamiento IPv6

La primera diferencia respecto a IPv4 es que las direcciones IPv6 son de 128 bits y están representadas en un formato hexadecimal en lugar de la notación decimal tradicional y separada cada parte por dos puntos en lugar de uno. Teniendo de esta forma 8 partes de 16 bits cada una. Como cada dígito hexadecimal se asocia con 4 bits, cada campo de 16 bits será de 4 dígitos hexadecimales.

Un ejemplo de dirección IPv6 puede ser el siguiente:

2001:0000:0001:0002:0000:0000:0000:ABCD

Este formato se puede reducir hasta de optimizar la lectura para su comprensión. Hay dos formas para conseguir simplificar tanta cantidad de números:

- Todos los 0 a la izquierda de cada uno de los campos pueden ser omitidos.

2001:0:1:2:0:0:0:ABCD

- Se pueden omitir los campos consecutivos de 0 con "::" independientemente de la cantidad de campos que se abrevie. Este

mecanismo solo puede hacerse una vez debido a que luego no se podrían reestructurar la cantidad de campos exactamente como eran.

2001:0:1:2::ABCD

1.15.2 Tipos de comunicación IPv6

De la misma manera que su antecesor, en IPv6 se soportan estas tres clases de direcciones:

- **Unicast**: para enviar tráfico a una sola interfaz.
- **Multicast**: para enviar a todas las interfaces del mismo grupo. Una dirección IPv6 del mismo grupo multicast identifica un conjunto de interfaces en diferentes dispositivos.
- **Anycast**: para enviar tráfico a la interfaz más cercana dentro de un grupo. Una dirección IPv6 de anycast también identifica un conjunto de interfaces en diferentes dispositivos, pero la diferencia de un paquete enviado a una dirección anycast es que dicho paquete está destinado al dispositivo más cercano. Esto será determinado por el protocolo de enrutamiento que se esté utilizando. Todos los nodos con la misma dirección de anycast deberán proporcionar el mismo servicio.

Una interfaz puede tener varias direcciones y de diferentes tipos. Los routers tienen que reconocer estas direcciones incluyendo las de anycast y multicast.

1.16 FUNDAMENTOS PARA EL EXAMEN

- Tenga una idea clara sobre las siete capas del modelo OSI, las funciones en la red para que se usan y los protocolos asociados a cada una.
- Analice las diferencias entre los dispositivos de cada capa del modelo OSI, cuáles son sus funciones y para qué se aplican en cada caso.
- Recuerde las posibles causas que pueden generar congestión en una LAN. Cómo, de ser posible, evitarlo.
- Tenga en cuenta las diferencias entre dominio de colisión y dominio de broadcast y los dispositivos asociados a cada uno.

- Recuerde la diferencia entre orientado a conexión y no orientado a conexión y los protocolos a que hacen referencia.

- Sepa diferenciar entre los tipos de cableado Ethernet y sus estándares, además de saber distinguir en cada caso cuál utilizar según los dispositivos a conectar.

- Tenga en cuenta las características, campos y tamaño de la trama Ethernet.

- Recuerde las funciones de cada capa del modelo jerárquico de Cisco, para qué se aplican y los dispositivos asociados.

- Recuerde las cuatro capas del modelo TCP/IP, sus funciones y los protocolos asociados a cada una.

- Sepa cuáles son las diferencias entre el modelo TCP/IP y el modelo OSI. Analice y compare sus capas.

- Tenga en cuenta las diferencias fundamentales entre TCP y UDP, control de flujo, ACK, ventanas y ventanas deslizantes.

- Memorice los rangos de cada una de las clases de redes, el direccionamiento reservado para uso privado.

- Ejercite el cálculo de subredes, VLMS y resúmenes de ruta.

Capítulo 2

ENRUTAMIENTO IP

2.1 DETERMINACIÓN DE RUTAS IP

Para que un dispositivo de capa tres pueda determinar la ruta hacia un destino debe tener conocimiento de las diferentes rutas hacia él y cómo hacerlo. El aprendizaje y la determinación de estas rutas se llevan a cabo mediante un proceso de enrutamiento dinámico a través de cálculos y algoritmos que se ejecutan en la red o enrutamiento estático ejecutado manualmente por el administrador o incluso ambos métodos.

La información de enrutamiento que el router aprende desde sus fuentes se coloca en su propia tabla de enrutamiento. El router se vale de esta tabla para determinar los puertos de salida que debe utilizar para retransmitir un paquete hasta su destino.

La tabla de enrutamiento es la fuente principal de información del router acerca de las redes. Si la red de destino está conectada directamente, el router ya sabrá el puerto que debe usar para reenviar paquetes. Si las redes de destino no están conectadas directamente, el router debe aprender y calcular la ruta más óptima a usar para reenviar paquetes a dichas redes. La tabla de enrutamiento se construye mediante uno de estos dos métodos o ambos:

- **Rutas estáticas**. Aprendidas por el router a través del administrador, que establece dicha ruta manualmente, quien también debe actualizar cuando tenga lugar un cambio en la topología.

- **Rutas dinámicas**. Rutas aprendidas automáticamente por el router a través de la información enviada por otros routers, una vez que el administrador ha configurado un protocolo de enrutamiento que permite el aprendizaje dinámico de rutas.

Para poder enrutar paquetes de información un router debe conocer lo siguiente:

- **Dirección de destino**: dirección a donde han de ser enviados los paquetes.
- **Fuentes de información**: fuente (otros routers) de donde el router aprende las rutas hasta los destinos especificados.
- **Descubrir las posibles rutas hacia el destino**: rutas iniciales posibles hasta los destinos deseados.
- **Seleccionar las mejores rutas**: determinar cuál es la mejor ruta hasta el destino especificado.
- **Mantener las tablas de enrutamiento actualizadas**: mantener conocimiento actualizado de las rutas al destino.

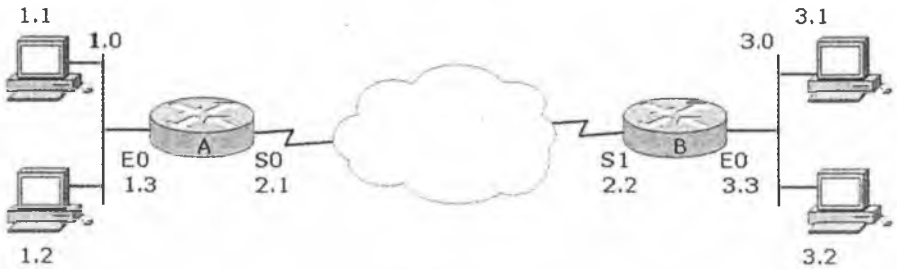


Tabla de enrutamiento Router A		
Red	Interfaz	Métrica
1	E0	0
2	S0	0
3	S0	1

Tabla de enrutamiento Router B		
Red	Interfaz	Métrica
1	S1	1
2	S1	0
3	E0	0

2.2 RUTAS ESTÁTICAS

Las rutas estáticas se definen administrativamente y establecen rutas específicas que han de seguir los paquetes para pasar de un puerto de origen hasta un puerto de destino. Se establece un control preciso del enrutamiento según los parámetros del administrador.

Las **rutas estáticas por defecto** (default) especifican una puerta de enlace (gateway) de último recurso, a la que el router debe enviar un paquete destinado a una red que no aparece en su tabla de enrutamiento, es decir, que desconoce.

Las rutas estáticas se utilizan habitualmente en enrutamientos desde una red hasta una red de conexión única, ya que no existe más que una ruta de entrada y salida en una red de conexión única, evitando de este modo la sobrecarga de tráfico que genera un protocolo de enrutamiento.

La ruta estática se configura para conseguir conectividad con un enlace de datos que no esté directamente conectado al router. Para conectividad de extremo a extremo, es necesario configurar la ruta en ambas direcciones. Las rutas estáticas permiten la construcción manual de la tabla de enrutamiento.

El comando **ip route** configura una ruta estática, los parámetros siguientes al comando definen la ruta estática.

Las entradas creadas en la tabla usando este procedimiento permanecerán en dicha tabla mientras la ruta siga activa. Con la opción **permanent**, la ruta seguirá en la tabla aunque la ruta en cuestión haya dejado de estar activa.

La sintaxis de configuración de una ruta estática es la siguiente:

```
Router(config)#ip route [red] [máscara] [dirección ip/interfaz]
[distancia] [permanent]
```

Donde:

- **red**: es la red o subred de destino.
- **máscara**: es la máscara de subred.
- **dirección**: es la dirección IP del router del próximo salto.
- **interfaz**: es el nombre de la interfaz que debe usarse para llegar a la red de destino.

- **distancia**: es un parámetro opcional, que define la distancia administrativa.

- **permanent**: un parámetro opcional que especifica que la ruta no debe ser eliminada, aunque la interfaz deje de estar activa.

NOTA:

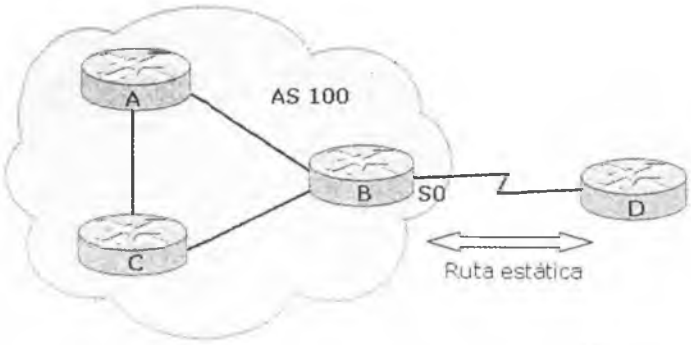
Es necesario configurar una ruta estática en sentido inverso para conseguir una comunicación en ambas direcciones.

2.2.1 Rutas estáticas por defecto

Una ruta estática por defecto (default), predeterminada o de último recurso es un tipo especial de ruta estática que se utiliza cuando no se conoce una ruta hasta un destino determinado, o cuando no es posible almacenar en la tabla de enrutamiento la información relativa a todas las rutas posibles.

La sintaxis de configuración de una ruta estática por defecto es la siguiente:

```
Router(config)#ip route 0.0.0.0 0.0.0.0 [dirección ip/interfaz]
[distancia]
```



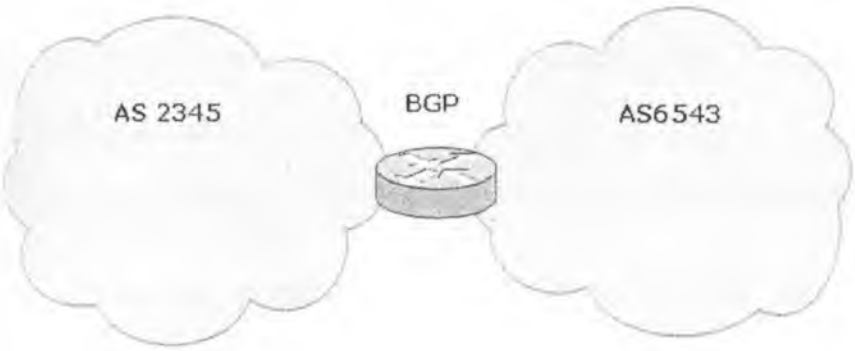

```
Router_B(config)# ip route 0.0.0.0 0.0.0.0 Serial 0
```

El gráfico ilustra un ejemplo de utilización de una ruta estática por default, el router B tiene configurada la ruta por defecto hacia el exterior como única

salida/entrada del sistema autónomo **100**, los demás routers aprenderán ese camino gracias a la redistribución que el protocolo hará dentro del sistema autónomo.

2.3 SISTEMA AUTÓNOMO

Un sistema autónomo (AS) es un conjunto de redes bajo un dominio administrativo común. El uso de números de sistema autónomos asignados por entidades (IANA, ARIN, RIPE...) solo es necesario si el sistema utiliza algún BGP, o una red pública como Internet.



Los sistemas autónomos intercambian información a través de protocolos de gateway exterior como BGP

2.4 DISTANCIA ADMINSTRATIVA

Los routers son multiprotocolos, lo que quiere decir que pueden utilizar al mismo tiempo diferentes protocolos incluidas rutas estáticas. Si varios protocolos proporçionan la misma información de enrutamiento se les debe otorgar un valor administrativo. La distancia administrativa permite que un protocolo tenga mayor prioridad sobre otro si su distancia administrativa es menor. Este valor viene por defecto, sin embargo el administrador puede configurar un valor diferente si así lo determina.

El rango de las distancias administrativas varía de 1 a 255 y se especifica en la siguiente tabla:

Interfaz	**0**
Ruta estática	**1**
Ruta sumarizada EIGRP	**5**
BGP externo	**20**
EIGRP interno	**90**
IGRP	**100**
OSPF	**110**
IS-IS	**115**
RIP	**120**
EIGRP externo	**170**
Inalcanzable	**255**

Valor predeterminado de distancia administrativa

2.5 PROTOCOLOS DE ENRUTAMIENTO

Los cambios que una red puede experimentar hacen poco factible la utilización de rutas estáticas, el administrador se vería forzado a reconfigurar los routers ante cada cambio. El enrutamiento dinámico permite que los routers actualicen conocimientos ante posibles cambios sin tener que recurrir a nuevas configuraciones. Un protocolo de enrutamiento permite determinar dinámicamente las rutas y mantener actualizadas sus tablas.

Es importante diferenciar los protocolos **enrutados** y los de **enrutamiento**. Un protocolo enrutado lleva una completa información de capa tres, como TCP/IP, IPX, APPLE TALK, Net BEUI. Un protocolo de enrutamiento es el utilizado por los routers para mantener tablas de enrutamiento y así poder elegir la mejor ruta hacia un destino.

Existen dos grandes núcleos de protocolos de enrutamiento:

- **Protocolos de gateway interior** (IGP). Se usan para intercambiar información de enrutamiento dentro de un sistema autónomo. (RIP, IGRP).

- **Protocolos de gateway exterior** (EGP). Se usan para intercambiar información de enrutamiento entre sistemas autónomos. (BGP).

2.5.1 Clases de protocolos de enrutamiento

Todos los protocolos de enrutamiento cumplen las mismas funciones, aprendiendo y determinando cuál es la mejor ruta hacia un destino.

Existen dos clases de protocolos de enrutamiento:

- **Vector distancia**: este tipo de protocolo determina la dirección y la distancia a cualquier red.

- **Estado de enlace**: estos protocolos poseen una idea exacta de la topología de la red y no efectúan actualizaciones a menos que ocurra un cambio en la topología.

Un tercer caso de protocolo de enrutamiento sería un método híbrido como es el caso de **EIGRP**, propietario de **Cisco**, que combina aspectos de los dos casos anteriores.

Un protocolo de enrutamiento también puede clasificarse como **classfull** (con clase) o **classless** (sin clase), es decir, que pueden no reconocer las máscaras de subred como en el caso de los classfull o sí pueden hacerlo en el caso de los classless.

Los routers que no pasan la información de las subredes son con clase, porque el router solo codifica la clase de red IP para la información de enrutamiento. En cuanto el direccionamiento IP fue adaptándose a las necesidades de crecimiento los protocolos se hicieron más sofisticados, pudiendo manipular máscaras de subred, estos protocolos son los llamados sin clase.

Un administrador puede habilitar el comando **ip classless** para el caso que se reciba un paquete hacia una subred desconocida, el router enviará ese paquete a la ruta predeterminada para enviar la trama al siguiente salto.

2.6 ENRUTAMIENTO POR VECTOR DISTANCIA

Los algoritmos de enrutamiento basados en vectores pasan copias periódicas de una tabla de enrutamiento de un router a otro y acumulan vectores de distancia. (Distancia es una medida de longitud, mientras que vector significa una dirección). Las actualizaciones regulares entre routers comunican los cambios en la topología. Cada protocolo de enrutamiento basado en vectores de distancia utiliza un algoritmo distinto para determinar la ruta óptima. El algoritmo genera un número, denominado métrica de ruta, para cada ruta existente a través de la red. Normalmente cuanto menor es este valor, mejor es la ruta.

Los dos ejemplos típicos de protocolos por vector distancia son:

- **RIP** (Protocolo de información de enrutamiento). Protocolo suministrado con los sistemas UNIX. Es el protocolo de gateway interior (IGP) más comúnmente utilizado. RIP utiliza el número de saltos como métrica de enrutamiento. Existen dos versiones, RIP v1 como protocolo tipo Classfull y RIP v2, más completo que su antecesor, como protocolo classless RIP se tratará con mayor detenimiento en los siguientes capítulos.

- **IGRP** (Protocolo de enrutamiento de gateway interior). Protocolo desarrollado por Cisco para tratar los problemas asociados con el enrutamiento en redes de gran envergadura. IGRP es un protocolo tipo classfull.

2.6.1 Métricas

Las métricas utilizadas habitualmente por los protocolos de enrutamiento pueden calcularse basándose en una sola o en múltiples características de la ruta.

- **Número de saltos**: número de routers por los que pasará un paquete.

- **Tic tac** (Novell): retraso en un enlace de datos usando pulsos de reloj de PC IBM (msg).

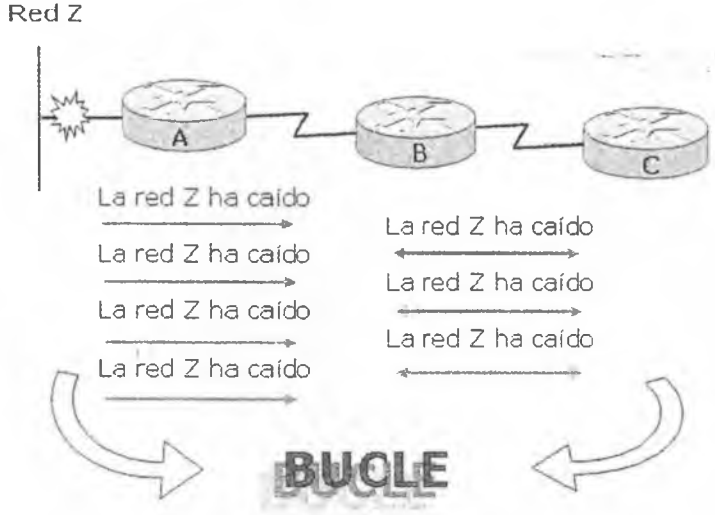
- **Coste**: valor arbitrario, basado generalmente en el ancho de banda, el coste económico u otra medida, que puede ser asignado por un administrador de red.

- **Ancho de banda**: capacidad de datos de un enlace. Por ejemplo, un enlace Ethernet de 10Mb será preferible normalmente a una línea dedicada de 64Kb.

- **Retraso**: tiempo en mover un paquete de un origen a un destino.
- **Carga**: cantidad de actividad existente en un recurso de red, como un router o un enlace.
- **Fiabilidad**: normalmente, se refiere al valor de errores de bits de cada enlace de red.
- **MTU** (Unidad Máxima de Transmisión): longitud máxima de trama en octetos que puede ser aceptada por todos los enlaces de la ruta.

2.7 BUCLES DE ENRUTAMIENTO

El proceso de mantener la información de enrutamiento puede generar errores si no existe una convergencia rápida y precisa entre los routers. En los diseños de redes complejas pueden producirse bucles o loops de enrutamiento. Los routers transmiten a sus vecinos actualizaciones constantes, si un router **A** recibe de **B** una actualización de una red que ha caído, este transmitirá dicha información a todos sus vecinos incluido el router **B**, quien primeramente le informó de la novedad, a su vez el router **B** volverá a comunicar que la red se ha caído al router **A** formándose un bucle interminable.

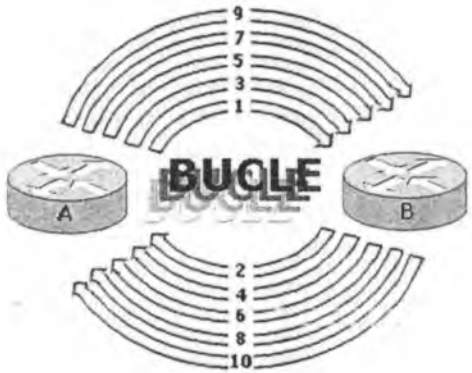


2.7.1 Solución a los bucles de enrutamiento

Los protocolos vector distancia poseen diferentes métodos para evitar los bucles de enrutamiento, generalmente estas herramientas funcionan por sí mismas (por defecto); sin embargo en algunos casos pueden desactivarse con el consiguiente riesgo que pudiera generar un bucle de red.

2.7.2 Métrica máxima

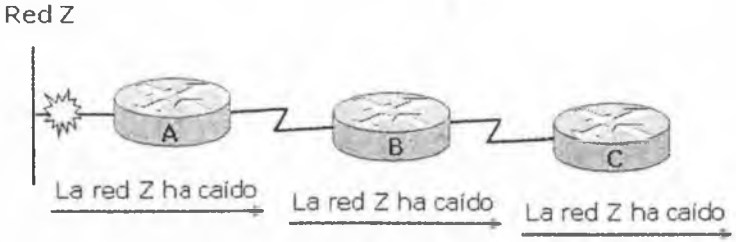
Un protocolo de enrutamiento permite la repetición del bucle de enrutamiento hasta que la métrica exceda del valor máximo permitido. Los routers agregan a la información de enrutamiento la cantidad de saltos transcurridos desde el origen a medida que los paquetes son enrutados. En el caso de RIP el bucle solo estará permitido hasta que la métrica llegue a 16 saltos.



Cuando el paquete sume 16 saltos será descartado por RIP

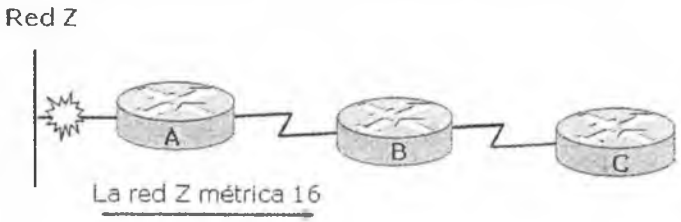
2.7.3 Horizonte dividido

Resulta sin sentido volver a enviar información acerca de una ruta a la dirección de donde ha venido la actualización original. A menos que el router conozca otra ruta viable al destino, **horizonte dividido** o **split horizon** no devolverá información por la interfaz donde la recibió.



2.7.4 Envenenamiento de rutas

El router crea una entrada en la tabla donde guarda el estado coherente de la red en tanto que otros routers convergen gradualmente y de forma correcta después de un cambio en la topología. La actualización inversa es una operación complementaria del horizonte dividido. El objetivo es asegurarse de que todos los routers del segmento hayan recibido información acerca de la ruta envenenada. El router agrega a la información de enrutamiento la cantidad máxima de saltos.



2.7.5 Temporizadores de espera

Los temporizadores hacen que los routers no apliquen ningún cambio que pudiera afectar a las rutas durante un periodo de tiempo determinado. Si llega una actualización con una métrica mejor a la red inaccesible, el router se actualiza y elimina el temporizador. Si no recibe cambios óptimos dará por caída la red al transcurrir el tiempo de espera.

2.8 ENRUTAMIENTO POR ESTADO DE ENLACE

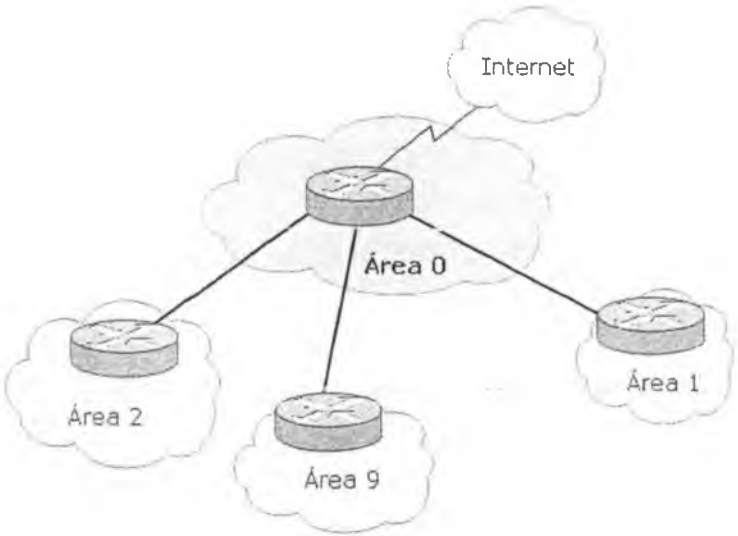
Los protocolos de estado de enlace construyen tablas de enrutamiento basándose en una base de datos de la topología. Esta base de datos se elabora a partir de paquetes de estado de enlace que se pasan entre todos los routers para describir el estado de una red.

El algoritmo **SPF** (primero la ruta libre más corta) usa una base de datos para construir la tabla de enrutamiento. El enrutamiento por estado de enlace utiliza la información resultante del árbol SFP, a partir de los paquetes de estado de enlace (LSP) creando una tabla de enrutamiento con las rutas y puertos de toda la red.

Los protocolos de enrutamiento por estado de enlace recopilan la información necesaria de todos los routers de la red, cada uno de los routers calcula de forma independiente su mejor ruta hacia un destino. De esta manera se producen muy pocos errores al tener una visión independiente de la red por cada router.

Estos protocolos prácticamente no tienen limitaciones de saltos. Cuando se produce un fallo en la red el router que detecta el error utiliza una dirección multicast para enviar una tabla LSA, cada router recibe y la reenvía a sus vecinos. La métrica utilizada se basa en el coste, que surge a partir del algoritmo de Dijkstra y se basa en la velocidad del enlace.

Los protocolos de estado de enlace son protocolos de enrutamiento de gateway interior, se utilizan dentro de un mismo **AS** (sistema autónomo) el que puede dividirse en sectores más pequeños como divisiones lógicas llamadas áreas. El **área 0** es el área principal del AS. Esta área también es conocida como **área de backbone**.



Jerarquía de estado de enlace dentro de un sistema autónomo

Los dos ejemplos típicos de protocolos de estado de enlace son:

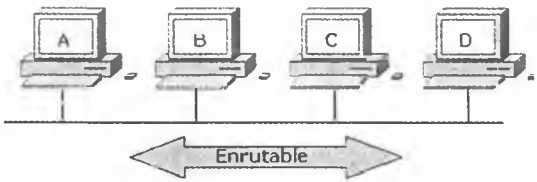
- **IS-IS** (Sistema Intermedio a Sistema Intermedio). Protocolo de enrutamiento jerárquico de estado de enlace casi en desuso hoy en día.

- **OSPF** (primero la ruta libre más corta). Protocolo de enrutamiento por estado de enlace jerárquico, que se ha propuesto como sucesor de RIP en la comunidad de Internet. Entre las características de OSPF se incluyen el enrutamiento de menor coste, el enrutamiento de múltiples rutas y el balanceo de carga.

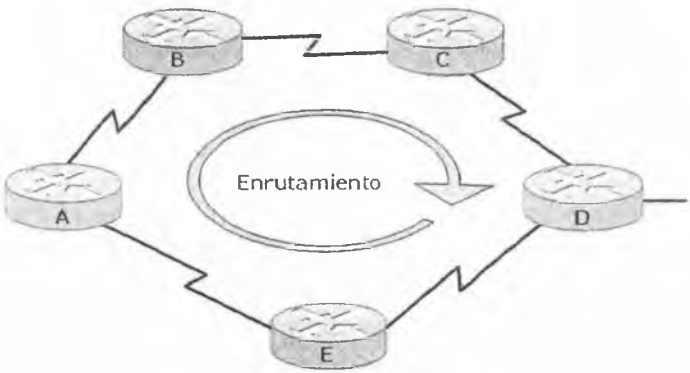
Los protocolos de estado de enlace son más rápidos y más escalables que los de vector distancia, algunas razones podrían ser:

- Los protocolos de estado de enlace solo envían actualizaciones cuando hay cambios en la topología.
- Las actualizaciones periódicas son menos frecuentes que en los protocolos por vector de distancia.
- Las redes que ejecutan protocolos de enrutamiento por estado de enlace pueden ser segmentadas en distintas áreas jerárquicamente organizadas, limitando así el alcance de los cambios de rutas.
- Las redes que ejecutan protocolos de enrutamiento por estado de enlace soportan direccionamiento sin clase.
- Las redes con protocolos de enrutamiento por estado de enlace soportan resúmenes de ruta.

RECUERDE:



Los protocolos enrutables son utilizados por los PC para poder "hablar" entre ellos



Los protocolos de enrutamiento son utilizados por los routers para poder "hablar" entre ellos

RECUERDE:

Protocolo	RIP	RIPv2	IGRP	EIGRP	IS-IS	OSPF
Vector distancia	X	X	X	X		
Estado de enlace					X	X
Resumen automático de ruta	X	X	X	X	X	
Resumen manual de ruta	X	X	X	X	X	X
Soporte VLSM		X		X	X	X
Propietario de Cisco			X	X		
Convergencia	Lento	Lento	Lento	Muy rápido	Muy rápido	Muy rápido
Distancia administrativa	120	120	100	90	115	110
Tiempo de actualización	30	30	90			
Métrica	Saltos	Saltos	Com-puesta	Com-puesta	Coste	Coste

NOTA:

El término convergencia hace referencia a la capacidad de los routers de poseer la misma información de enrutamiento actualizada. Las siglas VLSM son las de máscara de subred de longitud variable.

RECUERDE:

Mientras los campos IP se mantienen intactos a lo largo de la ruta, las tramas cambian en cada salto con la MAC correspondiente al salto siguiente.

2.9 FUNDAMENTOS PARA EL EXAMEN

- Tome en cuenta las diferencias entre rutas estáticas y dinámicas, aprendizaje de direcciones y cuál es la manera más adecuada para aplicarlas.
- Analice las condiciones básicas necesarias para la aplicación de rutas estáticas y rutas estáticas por defecto.
- Recuerde cuáles son los parámetros de configuración de las rutas estáticas y rutas estáticas por defecto.
- Recuerde qué es y para qué sirve un sistema autónomo.
- Recuerde qué es la distancia administrativa, su aplicación a los protocolos de enrutamiento y sus diferentes valores.
- Analice y asimile el funcionamiento de los protocolos de enrutamiento.
- Estudie cómo funciona un protocolo vector distancia, cuáles son y sus respectivas métricas.
- Analice la problemática de los bucles de enrutamientos y sus posibles soluciones razonando el funcionamiento de cada una de ellas.
- Estudie cómo funciona un protocolo de estado de enlace, cuáles son, sus jerarquías y compárelos con los de vector distancia.
- Recuerde la diferencia entre protocolos enrutables y de enrutamiento.

Capítulo 3

CONFIGURACIÓN INICIAL DEL ROUTER

3.1 PANORÁMICA DEL FUNCIONAMIENTO DEL ROUTER

Un router es un ordenador construido para desempeñar funciones específicas de capa tres, proporciona el hardware y software necesarios para encaminar paquetes entre redes. Se trata de dispositivos importantes de interconexión que permiten conectar subredes LAN y establecer conexiones de área amplia entre las subredes.

Las dos tareas principales son las de **conmutar** los paquetes desde una interfaz perteneciente a una red hacia otra interfaz de una red diferente y la de **enrutar**, es decir, encontrar el mejor camino hacia la red destino. Además de estas funciones los routers pueden llevar a cabo diferentes desempeños, tales como filtrados, dominios de colisión y broadcast, direccionamiento y traslación de direcciones IP, enlaces troncales, etc.

Además de los componentes de hardware los routers también necesitan un sistema operativo, los routers Cisco funcionan con un sistema operativo llamado **IOS** (Sistema operativo de internetworking). Un router puede ser exclusivamente un dispositivo **LAN**, o puede ser exclusivamente un dispositivo WAN, pero también puede estar en la frontera entre una LAN y una WAN y ser un dispositivo LAN y WAN al mismo tiempo.

3.1.1 Componentes principales de un router

Los componentes básicos de la arquitectura interna de un router comprenden:

- **CPU**. La unidad central de procesamiento (CPU) ejecuta las instrucciones del sistema operativo. Estas funciones incluyen la inicialización del sistema, las funciones de enrutamiento y el control de la interfaz de red. La CPU es un microprocesador. Los grandes routers pueden tener varias CPU.

- **RAM**. La memoria de acceso aleatorio (RAM) se usa para la información de las tablas de enrutamiento, el caché de conmutación rápida, la configuración actual y las colas de paquetes. En la mayoría de los routers, la RAM proporciona espacio de tiempo de ejecución para el software IOS de Cisco y sus subsistemas. El contenido de la RAM se pierde cuando se apaga la unidad. En general, la RAM es una memoria de acceso aleatorio dinámica (DRAM) y puede ampliarse agregando más módulos de memoria en línea doble (DIMM).

- **Memoria flash**. La memoria flash se utiliza para almacenar una imagen completa del software IOS de Cisco. Normalmente el router adquiere el IOS por defecto de la memoria flash. Estas imágenes pueden actualizarse cargando una nueva imagen en la memoria flash. El IOS puede estar comprimido o no. En la mayoría de los routers, una copia ejecutable del IOS se transfiere a la RAM durante el proceso de arranque. En otros routers, el IOS puede ejecutarse directamente desde la memoria flash. Agregando o reemplazando los módulos de memoria en línea simples flash (SIMM) o las tarjetas PCMCIA se puede ampliar la cantidad de memoria flash.

- **NVRAM**. La memoria de acceso aleatorio no volátil (NVRAM) se utiliza para guardar la configuración de inicio. En algunos dispositivos, la NVRAM se implementa utilizando distintas memorias de solo lectura programables, que se pueden borrar electrónicamente (EEPROM). En otros dispositivos, se implementa en el mismo dispositivo de memoria flash desde donde se cargó el código de arranque. En cualquiera de los casos, estos dispositivos retienen sus contenidos cuando se apaga la unidad.

- **Buses**. La mayoría de los routers contienen un bus de sistema y un bus de CPU. El bus de sistema se usa para la comunicación entre la CPU y las interfaces y/o ranuras de expansión. Este bus transfiere los paquetes

hacia y desde las interfaces. La CPU usa el bus para tener acceso a los componentes desde el almacenamiento del router. Este bus transfiere las instrucciones y los datos hacia o desde las direcciones de memoria especificadas.

- **ROM**. La memoria de solo lectura (ROM) se utiliza para almacenar de forma permanente el código de diagnóstico de inicio (Monitor de ROM). Las tareas principales de la ROM son el diagnóstico del hardware durante el arranque del router y la carga del software IOS de Cisco desde la memoria flash a la RAM. Algunos routers también tienen una versión más básica del IOS que puede usarse como fuente alternativa de arranque. Las memorias ROM no se pueden borrar. Solo pueden actualizarse reemplazando los chips de ROM en los routers.

- **Fuente de alimentación**. La fuente de alimentación brinda la energía necesaria para operar los componentes internos. Los routers de mayor tamaño pueden contar con varias fuentes de alimentación o fuentes modulares. En algunos de los routers de menor tamaño, la fuente de alimentación puede ser externa al router.

3.1.2 Interfaces

Las interfaces son las conexiones de los routers con el exterior. Los tres tipos de interfaces características son:

- Interfaz de red de área local (LAN).
- Interfaz de red de área amplia (WAN).
- Interfaz de consola/AUX.

Estas interfaces tienen chips controladores que proporcionan la lógica necesaria para conectar el sistema a los medios. Las interfaces LAN pueden ser configuraciones fijas o modulares y pueden ser Ethernet o Token Ring. Las interfaces WAN incluyen la Unidad de servicio de canal (CSU) integrada, la RDSI y la serial. Al igual que las interfaces LAN, las interfaces WAN también cuentan con chips controladores para las interfaces. Las interfaces WAN pueden ser de configuraciones fijas o modulares. Los puertos de consola/AUX son puertos seriales que se utilizan principalmente para la configuración inicial del router. Estos puertos no son puertos de networking. Se usan para realizar sesiones terminales desde los puertos de comunicación del ordenador o a través de un módem.

3.1.3 WAN y routers

La capa física WAN describe la interfaz entre el equipo terminal de datos (DTE) y el equipo de transmisión de datos (DCE). Normalmente el **DCE** es el proveedor del servicio, mientras que el **DTE** es el dispositivo conectado. En este modelo, los servicios ofrecidos al DTE están disponibles a través de un módem o **CSU/DSU**.

Cuando un router usa los protocolos y los estándares de la capa de enlace de datos y física asociados con las WAN, opera como dispositivo WAN.

Los protocolos y estándares de la capa física WAN son:

- EIA/TIA -232
- EIA/TIA -449
- V.24
- V.35
- X.21
- G.703
- EIA-530
- RDSI
- T1, T3, E1 y E3
- xDSL
- SONET (OC-3, OC-12, OC-48, OC-192)

Los protocolos y estándares de la capa de enlace de datos WAN:

- Control de enlace de datos de alto nivel (HDLC)
- Frame-Relay
- Protocolo punto a punto (PPP)
- Control de enlace de datos síncrono (SDLC)
- Protocolo Internet de enlace serial (SLIP)

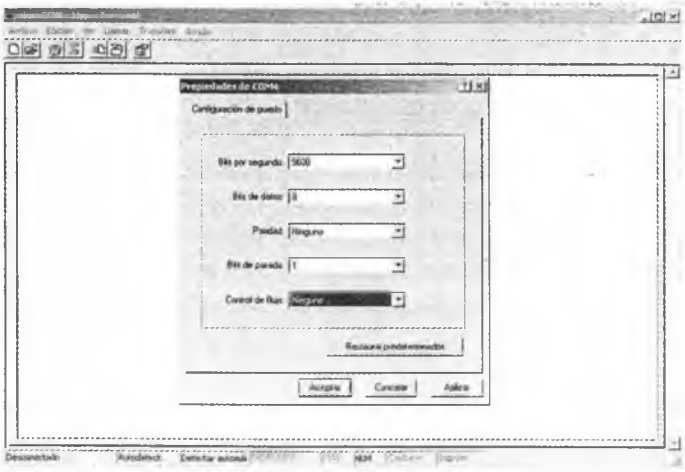
- X.25
- ATM
- LAPB
- LAPD
- LAPF

3.2 CONECTÁNDOSE POR PRIMERA VEZ AL ROUTER

Para la configuración inicial del router se utiliza el puerto de consola conectado a un cable transpuesto o de consola y un adaptador RJ-45 a DB-9 para conectarse al puerto **COM1** del ordenador. Este debe tener instalado un software de emulación de terminal, como el HyperTerminal.

Los parámetros de configuración son los siguientes:

- El puerto COM adecuado
- 9600 baudios
- 8 bits de datos
- Sin paridad
- 1 bit de parada
- Sin control de flujo



La imagen corresponde a una captura de pantalla de HyperTerminal

3.2.1 Secuencia de arranque

Cuando un router o un switch Catalyst Cisco se ponen en marcha, hay tres operaciones fundamentales que han de llevarse a cabo en el dispositivo de red:

- **Paso 1 -** El dispositivo localiza el hardware y lleva a cabo una serie de rutinas de detección del mismo. Un término que se suele utilizar para describir este conjunto inicial de rutinas el **POST** (*Power-on Self Test*), o pruebas de inicio.

- **Paso 2 -** Una vez que el hardware se muestra en una disposición correcta de funcionamiento, el dispositivo lleva a cabo rutinas de inicio del sistema. El switch o el router inicia localizando y cargando el software del sistema operativo **IOS** secuencialmente desde la **Flash**, servidor TFTP o la ROM, según corresponda.

- **Paso 3 -** Tras cargar el sistema operativo, el dispositivo trata de localizar y aplicar las opciones de configuración que definen los detalles necesarios para operar en la red. Generalmente, hay una secuencia de rutinas de arranque que proporcionan alternativas al inicio del software cuando es necesario.

3.3 CONFIGURACIÓN INICIAL

Un router o un switch pueden ser configurados desde distintas ubicaciones:

- En la instalación inicial, el administrador de la red configura generalmente los dispositivos de la red desde un terminal de consola, conectado por medio del puerto de consola.

- Si el administrador debe dar soporte a dispositivos remotos, una conexión local por módem con el puerto auxiliar del dispositivo permite a aquél configurar los dispositivos de red.

- Dispositivos con direcciones IP establecidas pueden permitir conexiones Telnet para la tarea de configuración.

- Descargar un archivo de configuración de un servidor Trivial File Transfer Protocol (TFTP).

- Configurar el dispositivo por medio de un navegador Hypertext Transfer Protocol (HTTP).

Las rutinas de inicio del software Cisco IOS tienen por objetivo inicializar las operaciones del router. Como se explicó anteriormente, las rutinas de puesta en marcha deben hacer lo siguiente:

- Asegurarse que el router cuenta con hardware verificado (POST).
- Localizar y cargar el software Cisco IOS que usa el router para su sistema operativo.
- Localizar y aplicar las instrucciones de configuración relativas a los atributos específicos del router, funciones del protocolo y direcciones de interfaz.

El router se asegura de que el hardware haya sido verificado. Cuando un router Cisco se enciende, realiza unas pruebas al inicio (POST). Durante este autotest, el router ejecuta una serie de diagnósticos para verificar la operatividad básica de la CPU, la memoria y la circuitería de la interfaz. Tras verificar que el hardware ha sido probado, el router procede con la inicialización del software.

Al iniciar por primera vez un router Cisco, no existe configuración inicial alguna. El software del router le pedirá un conjunto mínimo de detalles a través de un diálogo opcional llamado **Setup**.

El modo **Setup** es el modo en el que inicia un router no configurado al arrancar, puede mostrarse en su forma **básica** o **extendida**.

Se puede salir de este modo respondiendo que **NO** a la pregunta inicial.

```
Would you like to enter the initial configuration dialog?[yes]: No
Would you like to terminate autoinstall? [yes]: INTRO
```

Desde la línea de comandos el router se inicia en el modo EXEC usuario, las tareas que se pueden ejecutar en este modo son solo de verificación ya que NO se permiten cambios de configuración. En el modo **EXEC** privilegiado se realizan las tareas típicas de configuración.

Modo EXEC usuario:

```
Router>
```

Modo EXEC privilegiado:

```
Router#
```

Para pasar del modo usuario al privilegiado ejecute el comando **enable**, para regresar **disable**. Esto es posible porque no se ha configurado contraseña, de lo contrario sería requerida cada vez que se pasara al modo privilegiado.

```
Router>

Router>enable

Router#disable

Router>
```

Modo global y de interfaz:

```
Router>enable
Router#configure terminal
Router(config)#interface [tipo de interfaz][número]
Router(config)#interface ethernet 0
Router(config-if)#exit
Router(config)#exit
Router#
```

Para pasar del modo privilegiado al **global** debe introducir el comando configure terminal, para pasar del modo global al de **interfaz** ejecute interface ethernet 0, en este caso se ha elegido la ethernet 0. Para regresar un modo más atrás utilice el **exit** o **Control+Z** que lo llevará directamente al modo privilegiado.

NOTA:

La información que aparece entre corchetes después de una pregunta es la que el router sugiere como válida **...dialog? [yes]:** ***bastará con aceptar con un Intro.***

3.3.1 Comandos ayuda

El router da la posibilidad de ayudas pues resulta difícil memorizar todos los comandos disponibles, el signo de interrogación (?) y el tabulador del teclado nos brindan la ayuda necesaria a ese efecto. El tabulador completa los comandos que no recordamos completos o que no queremos escribir en su totalidad.

El signo **?** colocado inmediatamente después de un comando muestra todos los que comienzan con esas letras, colocado después de un espacio (barra **espaciadora+?**) lista todos los comandos que se pueden ejecutar en esa posición.

La ayuda se puede ejecutar desde cualquier modo:

```
Router#?
Exec commands:
  access-enable     Create a temporary Access-List entry
  access-template   Create a temporary Access-List entry
  bfe               For manual emergency modes setting
  clear             Reset functions
--More--

Router(config)#?
Configure commands:
        aaa         Authentication, Authorization and Accounting.
        alias       Create command alias
        appletalk   Appletalk global configuration commands
        arp         Set a static ARP entry
        banner      Define a login banner
        boot        Modify system boot parameters
 --More--
```

Inmediatamente o después de un espacio según la ayuda solicitada:

```
Router#sh?
Show

Router#show ?
  access-expression  List access expression
  access-lists       List access lists
  accounting         Accounting data for active sessions
  aliases            Display alias commands
 -More-


Router(config)#inte?
interface

Router(config)#interface ?
  CTunnel           CTunnel interface
  FastEthernet      FastEthernet IEEE 802.3
  GigabitEthernet   GigabitEthernet IEEE 802.3z
  Loopback          Loopback interface
  Null              Null interface
  Port-channel      Ethernet Channel of interfaces
  Tunnel            Tunnel interface
  Vif               PGM Multicast Host interface
  Vlan              Catalyst Vlans
  fcpa              Fiber Channel
  range             interface range command
```

La indicación —**More**— significa que existe más información disponible. La barra espaciadora pasará de página en página, mientras que el Intro lo hará línea por línea.

El acento circunflejo (^) indicará un fallo de escritura en un comando:

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

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

El uso de **Control+P** (también flecha hacia arriba) permite ver los últimos comandos ejecutados, el **Control-N** (también flecha hacia abajo) la inversa del anterior. Estos comandos quedan registrados en un búfer llamado historial y pueden verse con el comando **show history**, por defecto la cantidad de comandos que se guardan en memoria es de 10, pero puede ser modificado por el administrador utilizando el **history size**:

```
Router#terminal history size ?
<0-256>  Size of history buffer
```

3.3.2 Asignación de nombre y contraseñas

Se debe asignar un nombre exclusivo al router, como la primera tarea de configuración. Esto se realiza en el modo de configuración global, mediante los siguientes comandos:

```
Router(config)#hostname MADRID
MADRID(config)#
```

Los comandos **enable password** y **enable secret** se utilizan para restringir el acceso al modo EXEC privilegiado. El comando enable password se utiliza solo si no se ha configurado previamente enable secret.

Se recomienda habilitar siempre **enable secret**, ya que a diferencia de enable password, la contraseña estará siempre cifrada.

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

Observe en el ejemplo que se copia parte de un **show runnig-config** que se ha configurado como hostname del router **MADRID** y como contraseña **cisco** en la enable secret y la enable password, abajo se ve cómo la contraseña secret aparece encriptada por defecto mientras que la otra se lee perfectamente.

```
hostname MADRID
!
enable secret 5 $1$EBMD$0rTOiN4QQab7s8AFzsSof/
enable password cisco
```

3.3.3 Contraseñas de consola, auxiliar y telnet

Para configurar la contraseña para consola se debe acceder a la interfaz de consola con el comando **line console 0**:

```
Router#configure terminal
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password contraseña
```

El comando **exec-timeout** permite configurar un tiempo de desconexión determinado en la interfaz de consola.

El comando **logging synchronous** impedirá mensajes dirigidos a la consola de configuración que pueden resultar molestos.

Para configurar la contraseña para telnet se debe acceder a la interfaz de telnet con el comando **line vty 0 4**, donde line vty indica dicha interfaz, 0 el número de la interfaz y 4 la cantidad máxima de conexiones múltiples a partir de 0, en este caso se permiten 5 conexiones múltiples:

```
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password contraseña
```

El comando **show sessions** muestra las conexiones de telnet efectuadas desde el router, el comando **show users** muestra las conexiones de usuarios remotos.

```
Router#show users
    Line       User    Host(s)       Idle       Location
*   1 vty 0            idle          00:00:00   192.168.59.132
    2 vty 1            idle          00:00:02   192.168.59.156


  Interface      User     Mode        Idle     Peer Address
```

Algunos routers permiten establecer niveles de seguridad en la conexión por telnet y además de la configuración **ssh**.

```
Router(config)#line vty 0 15
Router(config-line)#privilege level 15
Router(config-line)#login local
Router(config-line)#transport input telnet
Router(config-line)#transport input telnet ssh
```

Para configurar la contraseña para auxiliar se debe acceder a la interfaz de auxiliar con el comando **line aux 0**:

```
Router(config)# line aux 0
Router(config-line)#login
Router(config-line)#password contraseña
```

En todos los casos el comando **login** suele estar configurado por defecto, permite que el router pregunte la contraseña al intentar conectarse, con el comando **login local** el router preguntará qué usuario intenta entrar y su respectiva contraseña. Para que esto funcione se deben crear nombres de usuarios y contraseña con el siguiente comando:

```
Router(config)#username usuario1 password contraseña1
Router(config)#username usuario2 password contraseña2
```

3.4 CASO PRÁCTICO

3.4.1 Configuración de usuario y contraseña

En el siguiente ejemplo se han creado dos usuarios **CORE_SUR** con una contraseña **Ansur** y **CORE_NOR** con una contraseña **Anort**. Se configura a continuación la línea de consola:

```
Router(config)#username CORE_SUR password Ansur
Router(config)#username CORE_NOR password Anort

Router#configure terminal
Router(config)#line console 0
Router(config-line)#login local
```

Cuando el usuario **CORE_NOR** intente ingresar al router le será solicitado su usuario y contraseña, y luego la enable secret:

```
Press RETURN to get started.

 Usted intenta ingresar en un sistema protegido

User Access Verification

Username: CORE_NOR
Password:***** (contraseña de usuario, Anort)
Router>enable
Password:***** (enable secret, cisco)
Router#
```

NOTA:

> ***Las contraseñas sin encriptación aparecen en el show running debiendo tener especial cuidado ante la presencia de intrusos.***

El comando **service password-encryption** encriptará con un cifrado leve las contraseñas que no están cifradas por defecto como las de telnet, consola, auxiliar, etc. Una vez cifradas las contraseñas no se podrán volver a leer en texto plano.

3.4.2 Configuración por navegador

Los routers pueden ser configurados por HTTP si el comando **ip http Server** está habilitado en el dispositivo. Por defecto la configuración por web viene deshabilitada por defecto (no ip http Server). Por razones de seguridad se recomienda dejarlo desactivado.

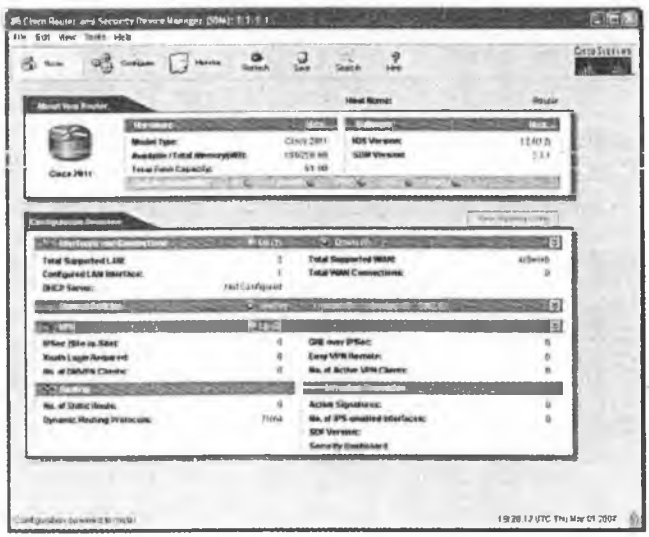
```
Router(config)#ip http Server
```

3.5 INTERFAZ SDM

SDM (*Cisco Router and Security Device Manager*) es una herramienta de administración avanzada muy potente que permite la configuración de los dispositivos en pocos minutos. Se basa en la configuración Web de los dispositivos siempre que estos tengan disponibles este servicio. SDM puede utilizarse en gran cantidad de modelos de routers y también se entrega preinstalado en todos los routers de servicios integrados nuevos de las series 850, 870, 1800, 2800 y 3800. Para un completo control administrativo de los dispositivos, SDM puede instalarse en un terminal de administración con la finalidad de gestionarlos desde allí.

Una vez instalado en el terminal de administración se puede acceder a los dispositivos introduciendo la dirección IP de los mismos. Otra forma es por medio de un navegador por HTTP o HTTPS.

SDM permite la revisión de las configuraciones, monitorizar y un espectro muy amplio de posibilidades de configuración rápida del dispositivo. Es posible efectuar configuraciones de todo tipo como por ejemplo NAT, VPN, ACL, contraseñas, protocolos, interfaces, etc.



Captura de una pantalla inicial del SDM

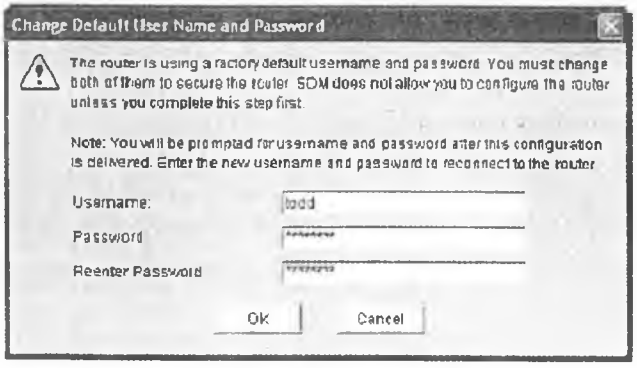
3.5.1 Configuración de SDM

Para la configuración de SDM es necesaria la instalación del software correspondiente suministrado por proveedor. Es posible la instalación tanto en los dispositivos como así también en el terminal de administración dependiendo de la utilidad y capacidad de memoria disponible.

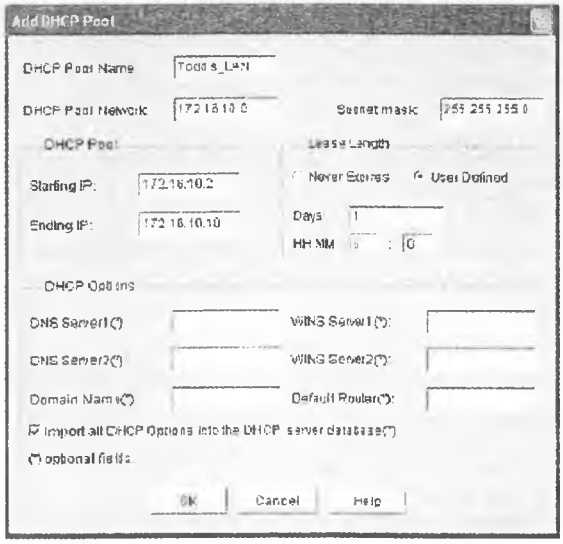
Es necesario activar el servicio HTTP o HTTPS en el router, crear el usuario y su contraseña con un nivel de privilegio 15. Tenga en cuenta que si es la configuración inicial y pretende continuar desde la terminal de administración debe existir por lo menos una interfaz activa en el router conectada a la red. Para ello verifique con un ping si es posible el acceso al dispositivo desde la terminal.

```
Router(config)#ip http server
Router(config)#ip http secure-server
Router(config)#ip http authentication local
Router(config)#username nombre usuario privilege 15 password 0
contraseña
```

SDM ofrece un abanico muy amplio de posibilidades de configuración, por ejemplo como muestran las siguientes imágenes, contraseñas o DHCP.



Captura de una pantalla del SDM para la configuración de contraseñas



Captura de una pantalla del SDM para la configuración de DHCP

3.6 CONFIGURACIÓN DE INTERFACES

Las interfaces de un router forman parte de las redes que están directamente conectadas al dispositivo. Estas interfaces activas deben llevar una dirección IP y su correspondiente máscara, como un host perteneciente a esa red. El administrador debe habilitar administrativamente la interfaz con el comando **no shutdown** y si fuera necesario la interfaz podrá deshabilitarse con el comando **shutdown**. Las **interfaces de LAN** pueden ser:

- Ethernet a 10 Mbpm.
- Fastethernet a 100 Mbpm.
- Gigaethernet a 1000 Mbpm.

Las secuencias de comandos para la configuración básica de una interfaz de LAN son los siguientes:

```
Router(config)#interface [tipo de interfaz] [número]
Router(config-if)#ip address [dirección IP máscara]
Router(config-if)#speed [10|100|1000|auto]
Router(config-if)#duplex [auto|full|half]
Router(config-if)#no shutdown
```

La mayoría de dispositivos llevan ranuras o slots donde se instalan las interfaces o para ampliar la cantidad de estas. Los slots están numerados y se configuran por delante del número de interfaz separado por una barra.

```
Router(config)#interface [tipo de interfaz][slot/int]
```

Es posible configurar en la interfaz un texto a modo de comentario que solo tendrá carácter informativo y que no afecta al funcionamiento del router. Puede tener cierta importancia para los administradores a la hora de solucionar problemas.

```
Router(config-if)#description comentario
```

El comando **show interfaces ethernet 0** muestra en la primera línea cómo la interfaz está **UP administrativamente** y **UP físicamente**. Recuerde que si la interfaz no estuviera conectada o si existiesen problemas de conectividad, el segundo **UP** aparecería como **down** o en un serial **down down**.

La tercera línea muestra la descripción configurada a modo de comentario. A continuación aparece la dirección IP, la encapsulación, paquetes enviados, recibidos, etc.

```
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 0000.0cfb.6c19 (bia 0000.0cfb.6c19)
  Description: INTERFAZ_DE_LAN
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 183/255, load
1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     188 packets output, 30385 bytes, 0 underruns
     188 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     188 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Si el administrador deshabilita la interfaz se verá:

```
Ethernet0 is administratively down, line protocol is down
Hardware is Lance, address is 0000.0cfb.6c19 (bia 0000.0cfb.6c19)
Description: INTERFAZ_DE_LAN
Internet address is 192.168.1.1/24
. . . . . .
```

NOTA:

Si una interfaz está administrativamente down no significa que exista un problema, pues el administrador ha decidido dejarla shutdown. Por el contrario si el line protocol is down existe un problema, seguramente de capa física.

Las **interfaces seriales** se configuran siguiendo el mismo proceso que las Ethernet, se debe tener especial cuidado para determinar quién es el **DCE** (equipo de comunicaciones) y quién el **DTE** (equipo terminal del abonado) debido a que el DCE lleva el sincronismo de la comunicación, este se configurará solo en la interfaz serial del DCE, el comando **clock rate** activará el sincronismo en ese enlace.

Clock rate y ancho de banda no es lo mismo: recuerde que existe un comando bandwidth para la configuración del ancho de banda, el router solo lo utilizará para el cálculo de costes y métricas para los protocolos de enrutamiento, mientras que el clock rate brinda la verdadera velocidad del enlace.

Las **interfaces loopback** son interfaces virtuales que sirven, por ejemplo, para el cálculo de métrica en los protocolos de enrutamiento.

3.7 COMANDOS SHOW

Saber utilizar e interpretar los comandos show permite el rápido diagnóstico de fallos, en modo usuario se permite la ejecución de los comandos show de forma restringida, desde el modo privilegiado la cantidad es ampliamente mayor.

3.7.1 Comandos show más usados

- **show interfaces**. Muestra las estadísticas completas de todas las interfaces del router. Para ver las de una interfaz específica, ejecute el comando seguido de la interfaz y el número de puerto.

```
Router#show interfaces serial 0/1
```

- **show controllers**. Muestra información específica de la interfaz de hardware.

```
Router#show controllers serial 0/1
```

- **show clock**. Muestra la hora fijada en el router.
- **show hosts**. Muestra la lista en caché de los nombres de host y sus direcciones.
- **show users**. Muestra todos los usuarios conectados al router.
- **show sessions**. Muestra las conexiones de telnet efectuadas desde el router.
- **show history**.Muestra un historial de los comandos introducidos.
- **show flash**. Muestra información acerca de la memoria flash (EEPROM) y qué archivos IOS se encuentran almacenados allí.
- **show version**. Despliega la información acerca del router y de la imagen de IOS que esté corriendo en la RAM. Este comando también muestra el valor del registro de configuración del router.
- **show arp**. Muestra la tabla ARP del router.
- **show protocols**. Muestra el estado global y por interfaz de cualquier protocolo de capa 3 que haya sido configurado.
- **show startup-config**. Muestra el archivo de configuración almacenado en la NVRAM.
- **show running-config**. Muestra el contenido del archivo de configuración activo o la configuración para una interfaz específica.

3.8 CASO PRÁCTICO

3.8.1 Configuración de una interfaz Ethernet

El ejemplo muestra la configuración de una interfaz Fastethernet:

```
Router>enable
Password:*******
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Fastethernet 0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#speed 100
Router(config-if)#duplex full
Router(config-if)#no shutdown
Router(config-if)#description INTERFAZ_DE_LAN
```

3.8.2 Configuración de una interfaz Serie

El ejemplo muestra la configuración de un enlace serial como **DCE**:

```
MADRID(config)#interface serial 0
MADRID(config-if)#ip address 170.16.2.1 255.255.0.0
MADRID(config-if)#clock rate 56000
MADRID(config-if)#bandwidth 100000
MADRID(config-if)#description RED_SERVIDORES
MADRID(config-if)#no shutdown
```

3.9 MENSAJES O BANNERS

Con el fin de brindar mensajes ante posibles averías o intrusos existen varios tipos de banners:

```
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
```

El **banner motd** ofrece la posibilidad de un mensaje diario, el **banner login** será visto al establecer una sesión de telnet, el **banner exec** al pasar la password al modo privilegiado.

Un mensaje de inicio de sesión debe advertir que solo los usuarios autorizados deben intentar el acceso. Evite un mensaje del estilo *¡bienvenido!* por el contrario deje bien claro que cualquier intrusión sin autorización estará penalizada por la ley vigente, de esta manera advertirá que ir más allá está prohibido y es ilegal.

Configuración de un banner diario, el texto debe ir entre caracteres similares al comenzar y al terminar:

```
Router(config)#banner motd * Usted intenta ingresar en un sistema
protegido*
```

3.10 RESOLUCIÓN DE NOMBRES DE HOST

Seguramente resultará más familiar identificar un dispositivo, un host o un servidor con un nombre que lo asocie a sus funciones o a otros criterios de desempeño. Esto se hace creando una tabla de host, que asociará un nombre a una o varias direcciones IP.

```
Router(config)#ip host nombre [1°dirección IP][2°dirección IP]...
```

3.11 CASO PRÁCTICO

3.11.1 Configuración de una tabla de host

A continuación se ha creado una tabla de host con el comando **ip host**.

```
Router(config)#ip host SERVIDOR 204.200.1.2
Router(config)#ip host ROUTER 220.220.10.32
Router(config)#ip host HOST 210.210.2.22
Router(config)#exit
```

3.12.1 Borrado del contenido de las memorias

Los datos de configuración almacenados en la memoria no volátil no son afectados por la falta de alimentación, el contenido permanecerá en la NVRAM hasta tanto se ejecute el comando apropiado para su eliminación:

```
Router#erase startup-config
```

Por el contrario no existe comando para borrar el contenido de la RAM. Si el administrador pretende dejar sin ningún dato de configuración debe rebotar o apagar el router. La RAM se borra únicamente ante la falta de alimentación eléctrica:

```
Router#reload
System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]
```

Para borrar completamente la configuración responda **NO** a la pregunta si quiere salvar.

NOTA:

Tenga especial cuidado al borrar las memorias, asegúrese de eliminar lo que desea antes de confirmar el borrado.

3.12.2 Copia de seguridad del IOS

Cuando sea necesario restaurar el IOS del router o actualizarlo se debe hacer desde un servidor TFTP. Es importante que se guarden copias de seguridad de todas las IOS en un servidor central.

El comando para esta tarea es el **copy flash tftp**, mediante el comando **show flash** se verificará el nombre del archivo a guardar:

```
Router#copy flash tftp

System flash directory:
File  Length   Name/status
  1   3709210  c4500-js-l_121-5.bin
[3709276 bytes used, 4679332 available, 8388608 total]
Address or name of remote host [255.255.255.255]? 200.200.10.1
Source file name? c4500-js-l_121-5.bin
```

```
Destination file name [c4500-js-l_121-5.bin]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Router#show flash

System flash directory:
File  Length    Name/status
  1   3709210   c4500-js-l_121-5.bin
[3709276 bytes used, 4679332 available, 8388608 total]
8192K bytes of processor board System flash (Read/Write)
```

En el proceso inverso al anterior o para actualizar el IOS se debe verificar el espacio en la memoria flash con el comando **show flash** y luego ejecutar el comando **copy tftp flash**:

```
Router#show flash

System flash directory:
File  Length    Name/status
  1   3709210   c4500-js-l_121-5.bin
[3709276 bytes used, 4679332 available, 8388608 total]
8192K bytes of processor board System flash (Read/Write)

      Router#copy tftp flash
Address or name of remote host?200.200.10.1
Source filename? c4500-js-l_121-5.bin
Destination filename [c4500-js-l_121-5.bin]?
Accessing tftp://200.200.10.1/ c4500-js-l_121-5.bin...
Erase flash: before copying? [confirm]
Erasing the flash file system will remove all files
Continue?[confirm]
Erasing device eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeee erased
Loading c4500-js-l_121-5.bin from 200.200.10.1 (via Ethernet 0/2)
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!
Verifying Check sum . . . . . OK
[OK-9024523 bytes]
9024523 bytes copied in 310.12 secs
```

3.13 COMANDOS DE EDICIÓN

Casi la totalidad de las IOS ofrecen combinaciones de teclas que permiten una configuración del dispositivo más rápida y simple. La siguiente tabla muestra algunos de los comandos de edición más utilizados.

Tecla	Efecto
Delete	Elimina un carácter a la derecha del cursor.
Retroceso	Elimina un carácter a la izquierda del cursor.
TAB	Completa un comando parcial.
Ctrl+A	Mueve el cursor al comienzo de la línea.
Ctrl+R	Vuelve a mostrar una línea escrita anteriormente.
Ctrl+U	Borra una línea.
Ctrl+W	Borra una palabra.
Ctrl+Z	Finaliza el modo de configuración y vuelve al modo EXEC.
Esc-B	Desplaza el cursor hacia atrás una palabra.
Flecha arriba	Repite hacia adelante los comandos anteriores.
Flecha abajo	Repite hacia atrás los comandos anteriores.
Ctrl+P	Repite hacia adelante los comandos anteriores
Ctrl+N	Repite hacia atrás los comandos anteriores.

3.14 NOMBRES DEL CISCO IOS

Cisco desarrolla numerosas versiones del **IOS** (*Internetwork Operating System*) y lanza nuevas versiones de forma continua.

El IOS ofrece diversas funciones y también corre sobre diversas plataformas de hardware.

Cisco ha establecido una convención para identificar por nombres a las distintas versiones, de los archivos del IOS. La convención de nombres del IOS utiliza varios campos. Entre ellos podemos mencionar el de identificación de la plataforma del hardware, el de identificación de la funcionalidad y el correspondiente a la secuencia numérica.

3.15 REGISTRO DE CONFIGURACIÓN

Cuando un router arranca, se comprueba el registro de configuración virtual para determinar (entre otras cosas) el modo en que debe entrar tras el arranque, dónde conseguir la imagen del software y cómo gestionar el archivo de configuración de la NVRAM.

Este registro de 16 bits controla funciones como la velocidad en baudios del puerto de la consola, la operación de carga del software, la habilitación o deshabilitación de la tecla de interrupción durante las operaciones normales, la dirección de multidifusión predeterminada, así como establecer una fuente para arrancar el router.

3.15.1 Comando show version

El comando **show version** muestra la información de hardware y de IOS de un router o switch, sobre las últimas líneas se observa el registro de configuración.

El valor del registro para una secuencia de arranque normal debe ser **0x2102** (el 0x indica un valor hexadecimal).

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 4000 Software (C4000-J-M), Version 11.2(21), RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 15-Dec-2004 23:15 by ccai
Image text-base: 0x00012000, data-base: 0x00775308
ROM: System Bootstrap, Version 5.2(11a), RELEASE SOFTWARE
ROM: 4000 Bootstrap Software (XX-RXBOOT), Version 10.2(11a), RELEASE
SOFTWARE (fc1)
Router uptime is 43 minutes
System restarted by power-on
System image file is "c4500-js-l_121-5.bin", booted via flash
cisco 4000 (68030) processor (revision 0xC0) with 32768K/16384K
bytes of memory.
Processor board ID 5050181
G.703/E1 software, Version 1.0.
Bridging software.
SuperLAT software copyright 1990 by Meridian Technology Corp).
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
TN3270 Emulation software.
2 Ethernet/IEEE 802.3 interface(s)
4 Serial network interface(s)
1 FDDI network interface(s)
128K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

Para cambiar el campo de arranque del registro de configuración, se hace desde el modo de configuración global, una vez ejecutado el comando se deberá reiniciar el router para que el cambio tenga efecto:

```
Router#configure terminal
Router(config)#config-register 0x2142
```

El valor del registro de configuración se ha cambiado a **0x2142**, observe el siguiente show, el registro solo funcionará al reiniciar el router. Tenga en cuenta que el router preguntará si se desea guardar los cambios a lo que se deberá responder **Yes** con el fin de que quede almacenada dicha modificación.

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 4000 Software (C4000-J-M), Version 11.2(21), RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 15-Dec-99 23:15 by ccai
Image text-base: 0x00012000, data-base: 0x00775308

ROM: System Bootstrap, Version 5.2(11a), RELEASE SOFTWARE
ROM: 4000 Bootstrap Software (XX-RXBOOT), Version 10.2(11a), RELEASE
SOFTWARE (fc1)
Router uptime is 1 hour, 1 minute
System restarted by power-on
System image file is "flash:y", booted via flash

cisco 4000 (68030) processor (revision 0xC0) with 32768K/16384K
bytes of memory.

Processor board ID 5050181
G.703/E1 software, Version 1.0.
Bridging software.
SuperLAT software copyright 1990 by Meridian Technology Corp).
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
TN3270 Emulation software.
2 Ethernet/IEEE 802.3 interface(s)
4 Serial network interface(s)
1 FDDI network interface(s)
128K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102 (will be 0x2142 at next reload)

Router#reload

System configuration has been modified. Save? [yes/no]: yes
Building configuration...
[OK]
Proceed with reload? [confirm]
```

Existen gran cantidad de opciones de valores de registros de configuración, los más importantes a tener en cuenta son los siguientes:

- Para entrar al modo de monitor de la ROM, configure como el valor del registro de configuración **0xnnn0**. Arranque el sistema operativo manualmente. Para ello ejecute el comando **b** al estar en pantalla el indicador del modo monitor de la ROM.

- Para arrancar usando la primera imagen en memoria **Flash**, o para arrancar usando el IOS en memoria **ROM** (dependiendo de la plataforma), fije el registro de configuración en **0xnnn1**.

- Para configurar el sistema de modo que arranque automáticamente desde la NVRAM, fije el registro de configuración en cualquier valor entre **0xnnn2** y **0xnnnF**. El uso de los comandos boot system almacenados en la NVRAM es el esquema por defecto.

3.16 RECUPERACIÓN DE CONTRASEÑAS

La recuperación de contraseñas le permite alcanzar el control administrativo de su dispositivo si ha perdido u olvidado su contraseña. Para lograr esto necesita conseguir acceso físico a su router, ingresar sin la contraseña, restaurar la configuración y restablecer la contraseña con un valor conocido.

3.16.1 Proceso para la recuperación de contraseña

Para routers Cisco:

- serie 2000
- serie 2500
- serie 3000
- serie 4000 con una CPU Motorola 680x0
- serie 7000 ejecutando Cisco IOS versión 10.0 o posterior

Siga estos pasos:

Paso 1 - Conecte un terminal o PC con software de emulación de terminal al puerto de consola del router. Acceda físicamente al router, apague y encienda el router.

Paso 2 - Pulse la tecla de interrupción del terminal durante los primeros 60 del encendido del router. En el caso de Hyperterminal la combinación del **control+pausa** dará la señal de interrupción en el router.

Aparecerá el símbolo > sin nombre del router. Si no aparece el símbolo, el terminal no está enviando la señal de interrupción correcta.

Paso 3 - Introduzca el comando **o/r 0x2142** (orden de registro) para arrancar desde la memoria Flash e ignorar la NVRAM.

Paso 4 - En el símbolo >, introduzca el comando **i** (initialize) para reiniciar el router. Esto hace que el router se reinicie pero ignore la configuración grabada en la NVRAM.

Paso 5 - Siga los pasos de arranque normales. Aparecerá el símbolo **router>**.

Paso 6 - La memoria RAM estará vacía, copie el contenido de la NVRAN a la RAM. De esta manera recuperará la configuración y también la contraseña no deseada. El nombre de router volverá a ser el original.

```
Router#copy startup-config running-config

MADRID#
```

Paso 7 - Cambie la contraseña no deseada por la conocida:

```
MADRID#configure terminal
MADRID (config)#enable secret Anort
```

Paso 8 - Guarde su nueva contraseña en la NVRAM, y si fuera necesario levante administrativamente las interfaces con el comando no shutdown:

```
MADRID#copy running-config startup-config
```

Paso 9 - Ejecute desde el modo global el comando **config-register 0x2102**.

Paso 10 - Introduzca el comando reload en el símbolo del nivel EXEC privilegiado. Responda Yes a la pregunta para guardar el registro de configuración y confirme el reinicio:

```
MADRID#reload

System configuration has been modified. Save? [yes/no]: yes
Building configuration...
[OK]
Proceed with reload? [confirm]
```

El router arrancará con la configuración y la contraseña conocida.

Para routers Cisco:

- serie 1700
- serie 2600
- serie 4500
- serie 7200
- serie 7500

Siga estos pasos:

Paso 1 - Conecte un terminal o PC con software de emulación de terminal al puerto de consola del router. Acceda físicamente al router, apague y encienda el router.

Paso 2 - Pulse la tecla de interrupción del terminal durante los primeros sesenta segundos del encendido del router. En el caso de Hyperterminal la combinación del **control+pausa** dará la señal de interrupción en el router. Aparecerá el símbolo **rommon>**. Si no aparece, el terminal no está enviando la señal de interrupción correcta. En este caso, compruebe la configuración del terminal o del emulador de terminal.

Paso 3 - Introduzca el comando **confreg 0x2142** en el símbolo **rommon>** para arrancar desde la memoria flash e ignorar la NVRAM.

Paso 4 - En el símbolo **rommon>** introduzca el comando **reset** para reiniciar el router. Esto hace que el router se reinicie pero ignore la configuración grabada en la NVRAM.

Paso 5 - Siga los pasos de arranque normales. Aparecerá el símbolo **router>**.

Paso 6 - La memoria RAM estará vacía, copie el contenido de la NVRAN a la RAM. De esta manera recuperará la configuración y también la contraseña no deseada. El nombre de router volverá a ser el original.

```
Router#copy startup-config running-config

MADRID#
```

Paso 7 - Cambie la contraseña no deseada por la conocida:

```
MADRID#configure terminal
```

```
MADRID (config)#enable secret Anort
```

Paso 8 - Guarde su nueva contraseña en la NVRAM, y si fuera necesario levante administrativamente las interfaces con el comando **no shutdown**:

```
MADRID#copy running-config startup-config
```

Paso 9 - Introduzca desde el modo global el comando **config-register 0x2102**.

Paso 10 - Introduzca el comando **reload** en el símbolo del nivel EXEC privilegiado. Responda Yes a la pregunta para guardar el registro de configuración y confirme el reinicio:

```
MADRID#reload
System configuration has been modified. Save? [yes/no]: yes
Building configuration...
[OK]
Proceed with reload? [confirm]
```

3.17 COMANDOS BOOT SYSTEM

Los comandos boot system especifican el nombre y la ubicación de la imagen IOS que se debe cargar.

```
Router(config)#boot system flash nombre_archivo
```

Indica al router que debe arrancar utilizando la IOS que está ubicada en la memoria flash.

```
Router(config)#boot system rom
```

Indica al router que debe buscar la IOS en la memoria ROM.

```
Router(config)#boot system tftp nombre_archivo [dirección_servidor]
```

Indica al router que al arrancar ha de cargar la imagen IOS de un servidor TFTP.

NOTA:

Si no existen comandos boot system en la configuración, el router carga por omisión el primer archivo encontrado en la memoria flash y la ejecuta.

3.18 PROTOCOLO CDP

El protocolo **CDP** (Cisco Discovery Protocol) se utiliza para obtener información de router y switches que están conectados localmente. El CDP es un protocolo propietario de Cisco, destinado al descubrimiento de vecinos y es independiente de los medios y del protocolo de enrutamiento. Aunque el CDP solamente mostrará información sobre los vecinos conectados de forma directa, constituye una herramienta de gran utilidad.

El Protocolo de descubrimiento de Cisco (CDP) es un protocolo de capa 2 que conecta los medios físicos inferiores con los protocolos de red de las capas superiores. CDP viene habilitado por defecto en los dispositivos Cisco, los dispositivos de otras marcas serán transparentes para el protocolo. CDP envía actualizaciones por defecto cada 60 segundos y un tiempo de espera antes de dar por caído al vecino (holdtime) de 180 segundos.

Como se explicó anteriormente CDP viene habilitado por defecto, sin embargo si fuera necesario configurarlo se ejecuta desde el modo global:

```
Router(config)#cdp run
```

Hay dos formas de deshabilitar CDP, una es en una interfaz específica para que no funcione particularmente con las conexiones locales y la otra de forma general para que no funcione completamente en ninguna interfaz. Las sintaxis muestran los respectivos comandos desde una interfaz y de modo total.

```
Router#configure terminal
Router(config)#[número de interfaz]
Router(config-if)#no cdp enable

Router(config)#no cdp run
```

El ajuste de los temporizadores se realiza con los siguientes comandos.

```
Router(config)#cdp timer [segundos]
Router(config)#cdp holdtime [segundos]
```

La lectura del comando **show cdp neighbors detail** es idéntica al **show cdp entry** * e incluye la siguiente información bien detallada:

- Dirección IP del router vecino.
- Información del protocolo.
- Plataforma.
- Capacidad.

- ID del puerto.
- Tiempo de espera.
- La ID del dispositivo vecino.
- La interfaz local.

Los siguientes datos se agregan en el CDPv2:

- Administración de nombres de dominio VTP.
- VLAN nativas.
- Full o half-duplex.

3.18.1 Verificación CDP

- **Show cdp neighbors**. Para obtener los nombres y tipos de plataforma de routers vecinos, nombres y versión de IOS.

- **Show cdp neighbors detail**. Para obtener datos de routers vecinos con más detalle.

- **Router#show cdp traffic**. Para saber el tráfico de CDP en el router.

- **Show cdp interface**. Muestra el estado de todos las interfaces que tienen activado CDP.

- **Router#clear cdp counters**. Restaura los contadores a cero.

- **Router#clear cdp table**. Borra la información contenida en la tabla de vecinos.

Los siguientes comandos pueden utilizarse para mostrar la versión, la información de actualización, las tablas y el tráfico:

- **show cdp traffic**
- **show debugging**
- **debug cdp adjacency**
- **debug cdp events**
- **debug cdp ip**
- **debug cdp packets**
- **cdp timer**
- **cdp holdtime**
- **show cdp**

Ejemplo de un **show cdp neighbors**:

```
Router#show cdp neighbors
Capability Codes: R-Router, T-Trans Bridge, B-Sourse
Route Bridge, S-Switch, H-Host, I-IGMP, r-Repeater

DeviceID  Local Interfce  Holdtme Capablyt Plataform Port ID
Router3   Ser0/1          150     R           2600    Ser0/1
Router4   Ser0/0          142     R           4500    Ser1/0
SWITCH    FASTET0/0       120     S           2950    FAST0/5
```

3.19 DHCP

DHCP (*Dynamic Host Control Protocol*) desciende del antiguo protocolo **BootP**, permite a un servidor asignar automáticamente a un host direcciones IPv4 y otros parámetros cuando está iniciándose. DHCP ofrece dos principales ventajas:

- DHCP permite que la administración de la red sea más fácil y versátil, evitando asignar manualmente el direccionamiento a todos los host, tarea bastante tediosa y que generalmente conlleva errores.

- DHCP asigna direcciones IP de manera temporal creando un mayor aprovechamiento del espacio en el direccionamiento.

El proceso DHCP sigue los siguientes pasos:

1. El cliente envía un broadcast preguntando por configuración IP a los servidores, **DHCP discover**.

2. Cada servidor en la red responderá con un **Offer**.

3. El cliente considera todas las ofertas y elije una. A partir de este momento el cliente envía un mensaje llamado **Request**.

4. El servidor responde con un **ACK** informando a su vez que toma conocimiento que el cliente se queda con esa dirección IP.

5. Finalmente el cliente envía un **ARP request** para esa nueva dirección IP. Si alguien responde, el cliente sabrá que esa dirección está en uso y que ha sido asignada a otro cliente lo que iniciará el proceso DHCP nuevamente. Este paso se llama **Gratuitous ARP**.

Cuando se detecta un host con una dirección IP 169.254.X.X significa que no ha podido contactar con el servidor DHCP.

3.20 CONFIGURACIÓN DHCP

3.20.1 Configuración del servidor

Los siguientes pasos describen la configuración de un router ejecutando IOS como servidor DHCP:

1. Crear un almacén (pool) de direcciones asignables a los clientes.

```
Router(config)# ip dhcp pool nombre del pool
```

2. Determinar el direccionamiento de red y máscara para dicho pool.

```
Router(config-dhcp)# network [dirección IP-máscara]
```

3. Configurar el período que el cliente podrá disponer de esta dirección.

```
Router(config-dhcp)# lease [tiempo estipulado]
```

4. Identificar el servidor DNS.

```
Router(config-dhcp)# dns-server [dirección IP]
```

5. Identificar la puerta de enlace o gateway.

```
Router(config-dhcp)# default-router [dirección IP]
```

6. Excluir si es necesario las direcciones que por seguridad o para evitar conflictos no se necesita que el DHCP otorgue.

```
Router(config)#ip dhcp excluded-address [IP inicio-IP fin]
```

Las direcciones IP son siempre asignadas en la misma interfaz que tiene una IP dentro de ese pool. La siguiente sintaxis muestra un ejemplo de configuración dentro de ese contexto:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config)# ip dhcp pool 1
Router(config-dhcp)# network 192.168.1.0 /24
Router(config-dhcp)# default-router 192.168.1.1
Router(config-dhcp)# lease 3
Router(config-dhcp)# dns-server 192.168.77.100
```

Algunos dispositivos IOS reciben direccionamiento IP en algunas interfaces y asignan direcciones IP en otras. Para estos casos DHCP puede importar las opciones y parámetros de una interfaz a otra. El siguiente comando para ejecutar esta acción es:

```
Router(config-dhcp)# import all
```

Este comando es muy útil cuando se debe configurar DHCP en oficinas remotas. El router una vez localizado en su sitio puede determinar el DNS y las opciones locales.

3.20.2 Configuración de un DHCP Relay

Un router configurado para dejar pasar los **DHCP request** es llamado **DHCP Relay**. Cuando es configurado, el router permitirá el reenvío de broadcast que haya sido enviado a un puerto UDP determinado hacia una localización remota. El DHCP Relay reenvía los *requests* y configura la puerta de enlace en el router local.

```
Router(config-if)# ip helper-address [dirección IP]
```

3.20.3 Configuración de un cliente DHCP

Configurar IOS para la opción del DHCP como cliente es simple.

```
Router(config)# interface fastethernet0/0
Router(config-if)# ip address dhcp
```

Un router puede ser cliente, servidor o ambos a la vez en diferentes interfaces.

3.21 HERRAMIENTAS DE DIAGNÓSTICO

La correcta utilización de todos los comandos **show** descritos a lo largo de todo este libro permiten diagnosticar fallos de cualquier tipo en la Red. Su buena lectura y comprensión darán sus frutos a la hora de determinar y diagnosticar errores.

El protocolo **ICMP** (Protocolo de mensajes de control en Internet), suministra capacidades de control y envío de mensajes. Herramientas tales como **ping** y **trace** utilizan ICMP para poder funcionar, enviando un paquete a la dirección destino específica y esperando una determinada respuesta.

El comando **ping** prueba conectividad de sitio a sitio, en sus dos formas, básica y extendida, enviando y recibiendo paquetes **echo** según muestran las siguientes sintaxis.

```
Router>ping 10.99.60.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.99.60.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/16
ms

router#ping
Protocol [ip]: ip
Target IP address: 10.99.60.1
Repeat count [5]: 50
Datagram size [100]: 100
Timeout in seconds [2]: 2
Extended commands [n]: n
Sweep range of sizes [n]: n
Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 10.99.60.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 1/2/4
ms
```

La versión extendida del comando **ping** permite efectuar variantes tales como cantidad y tamaño de paquetes, tiempo entre cada envío, etc. Es una eficaz herramienta de pruebas cuando se desea no solo pruebas de conectividad sino también de carga.

La siguiente tabla muestra algunos de los caracteres con los que ping muestra efectividad o fallos.

Carácter	Descripción
!	Cada signo de exclamación indica la recepción de una respuesta.
.	Cada punto indica agotado el tiempo esperando por una respuesta.
U	Una PDU hacia el destino resulta inalcanzable.

Q	Destino muy congestionado.
?	Tipo de paquete desconocido.
&	Curso de vida de los paquetes se ha superado.

El comando **traceroute** utiliza el principio de funcionamiento del ping pero mostrando e identificando cada salto a lo largo de la ruta. Cuando un paquete **echo reply** (ping) no llega a su destino **traceroute** mostrará el salto donde dicho paquete no consigue llegar. En rutas extremadamente grandes la traza puede abortarse con las teclas **Ctrl+Shift+6**.

```
route#traceroute 10.99.60.1

Type escape sequence to abort.
Tracing the route to 10.99.60.1

      1 10.99.170.11 0 msec 0 msec 4 msec
      2 81.46.16.48 4 msec 0 msec 4 msec
      3 10.99.60.1 4 msec 0 msec 0 msec
```

Desde un router o switch es posible acceder a varias sesiones de Telnet a la vez, para poder realizar tareas de monitorización y diagnóstico. Por defecto, los dispositivos Cisco apuntan al puerto 23, las siguientes sintaxis muestran esta similitud.

```
Router#telnet 10.55.60.1
```

O lo que es lo mismo.

```
Router#10.55.60.1
```

Las diferentes sesiones de Telnet abiertas en un router pueden conmutarse con la secuencia de teclas **Ctrl+Shift+6** y luego **x** regresar con 2 veces **intro**.

El comando **show sessions** permite ver las sesiones abiertas hacia dispositivos remotos, mientras que el comando **show users** muestra las sesiones abiertas en el dispositivo local.

```
Router# show sessions

Conn Host              Address           Byte    Idle  Conn Name
   1 Administ          192.168.7.21         0       0  Administ
*  2 Jefatura          172.25.12.19         0       0  Jefatura


Router#show users
    Line       User    Host(s)       Idle        Location
*   1 vty 0            idle          00:00:00    192.168.59.132
    2 vty 1            idle          00:00:02    192.168.59.156


  Interface      User     Mode        Idle      Peer Address
```

El comando **clear line** desactivará una sesión de Telnet indeseada. Desde una conexión de consola, puede ejecutarse el comando **disconnet** para cancelar una conexión de un router remoto.

Una vez realizadas las pruebas ejecute un **show ip route** para verificar el contenido en su tabla de enrutamiento de todas las redes afectadas.

3.22 FUNDAMENTOS PARA EL EXAMEN

- Recuerde los componentes principales del router, sus funciones e importancia dentro de su arquitectura.
- Estudie y relacione los estándares de WAN con el router.
- Memorice los parámetros de configuración del emulador de consola para ingresar por primera vez al router.
- Analice los pasos de arranque del router, estudie la secuencia y para qué sirve cada uno de los pasos.
- Familiarícese con todos los comandos básicos del router, tenga en cuenta que le servirán para el resto de las configuraciones más adelante.
- Recuerde los comandos show más usados, habitúese a su utilización para detectar y visualizar incidencias o configuraciones.
- Estudie y analice las propiedades de las distintas interfaces que puede contener el router, recuerde los pasos a seguir en el proceso de configuración de cada una de ellas.

- Recuerde los comandos necesarios para efectuar copias de seguridad, los requisitos mínimos y los pasos para cargar desde diferentes fuentes. Tenga en cuenta las diferencias entre startup-config y running-config.
- Memorice los términos que componen el nombre del Cisco IOS.
- Tenga en cuenta la importancia del comando show version y los diferentes valores que puede tomar el registro de configuración.
- Recuerde los pasos en el proceso de recuperación de contraseñas y para qué sirve cada uno de ellos. Tenga una idea clara de cuáles son los registros de configuración antes y después de la recuperación.
- Recuerde la función y comandos del CDP, qué muestran y para qué se utilizan.
- Configure una topología con DHCP, observe los resultados y analícelos.
- Ejercite todas las configuraciones en dispositivos reales o en simuladores.
- Ejecute pruebas de conectividad con los comandos **ping** y **traceroute**, saque conclusiones.

Capítulo 4

ENRUTAMIENTO BÁSICO

4.1 CONFIGURACIÓN DE ENRUTAMIENTO IP

Para que un dispositivo de capa tres pueda determinar la ruta hacia un destino debe tener conocimiento de las diferentes rutas hacia él y cómo hacerlo. El aprendizaje y la determinación de estas rutas se llevan a cabo mediante un proceso de enrutamiento dinámico a través de cálculos y algoritmos que se ejecutan en la red o enrutamiento estático ejecutado manualmente por el administrador o incluso ambos métodos.

4.1.1 Enrutamiento estático

La configuración de las rutas estáticas se realiza a través del comando de configuración global de IOS ip route. El comando utiliza varios parámetros, entre los que se incluyen la dirección de red y la máscara de red asociada, así como información acerca del lugar al que deberían enviarse los paquetes destinados para dicha red.

La información de destino puede adoptar una de las siguientes formas:

- Una dirección IP específica del siguiente router de la ruta.
- La dirección de red de otra ruta de la tabla de enrutamiento a la que deben reenviarse los paquetes.

- Una interfaz conectada directamente en la que se encuentra la red de destino.

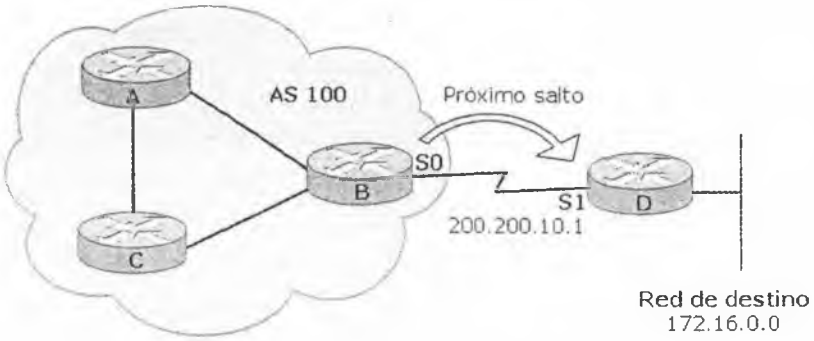
```
Router(config)#ip route [dirección IP de la red destino +
máscara] [IP del primer salto/interfaz de salida] [distancia
administrativa]
```

Donde:

- **dirección IP de la red destino+máscara**: hace referencia a la red a la que se pretende tener acceso y su correspondiente máscara de red o subred. Si el destino es un host específico se debe identificar la red a la que pertenece dicho host.

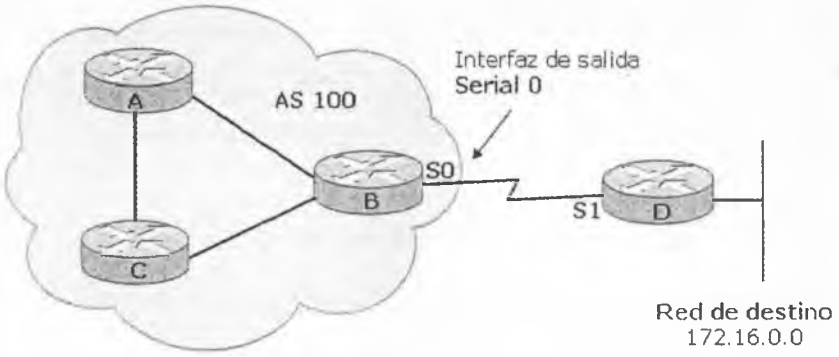
- **IP del primer salto/interfaz de salida**: se debe elegir entre configurar la IP del próximo salto (hace referencia a la dirección IP de la interfaz del siguiente router) o el nombre de la interfaz del propio router por donde saldrán los paquetes hacia el destino. Por ejemplo, si el administrador no conoce o tiene dudas acerca del próximo salto utilizará su propia interfaz de salida, de lo contrario es conveniente hacerlo con la IP del próximo salto.

- **distancia administrativa**: parámetro opcional (de 1 a 255) que si no se configura será igual a 1. Este valor hará que si existen más rutas estáticas o protocolos de enrutamiento configurados en el router cada uno de estos tendrá mayor o menor importancia según sea el valor de su distancia administrativa. Cuanto más baja, mayor importancia.




```
Router_B(config)#ip route 172.16.0.0 255.255.0.0 200.200.10.1 120
```

La sintaxis que se muestra apunta a la red 172.16.0.0 saliendo por el próximo salto 200.200.10.1 con una distancia administrativa de 120.




```
Router_B(config)#ip route 172.16.0.0 255.255.0.0 serial 0 120
```

La sintaxis que se muestra apunta a la red 172.16.0.0 saliendo por la interfaz serial 0 del propio router con una distancia administrativa de 120.

4.1.2 Situaciones en las que se aconsejan las rutas estáticas

- Un circuito de datos es especialmente poco fiable y deja de funcionar constantemente. En estas circunstancias, un protocolo de enrutamiento dinámico podrá producir demasiada inestabilidad, mientras que las rutas estáticas no cambian.

- Existe una sola conexión con un solo ISP. En lugar de conocer todas las rutas globales de Internet, se utiliza una sola ruta estática.

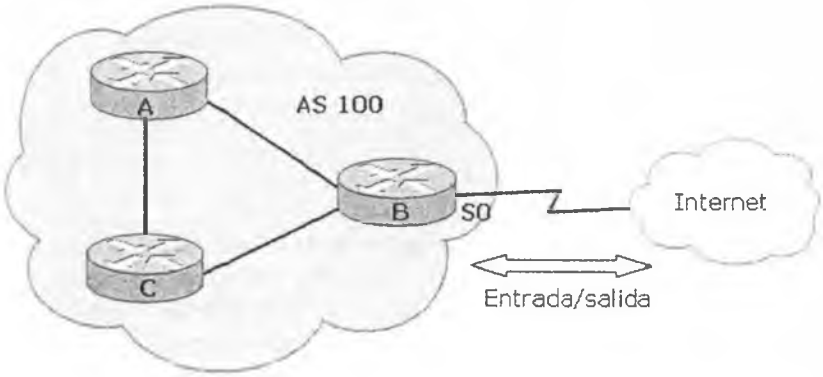
- Se puede acceder a una red a través de una conexión de acceso telefónico. Dicha red no puede proporcionar las actualizaciones constantes que requieren un protocolo de enrutamiento dinámico.

- Un cliente o cualquier otra red vinculada no desean intercambiar información de enrutamiento dinámico. Se puede utilizar una ruta estática para proporcionar información acerca de la disponibilidad de dicha red.

4.1.3 Configuración de rutas estáticas por defecto

Cuando el destino al que se pretende llegar son múltiples redes o no se conocen se pueden crear rutas estáticas por defecto como lo muestra la siguiente sintaxis:

```
Router(config)#ip route 0.0.0.0 0.0.0.0[IP del primer salto/interfaz
de salida][distancia administrativa]
```




```
Router_B(config)#ip route 0.0.0.0 0.0.0.0 serial 0
```

Observe que los parámetros de configuración en lugar de una dirección de red específica de destino se utilizan ceros en los octetos de red y máscara, el resto de los parámetros serán iguales a las rutas estáticas convencionales.

RECUERDE:

Cuando configure una ruta de red predeterminada, siga estas directrices importantes:

- Si la información de enrutamiento dinámico no se intercambia con la entidad externa, como un IPS, el uso de una ruta estática suele ser la forma más fácil de generar una ruta predeterminada.

- Si la información de enrutamiento dinámico no se intercambia con uno o varios IPS, el uso del comando **ip default-network** es la forma más apropiada de designar una o varias rutas de red predeterminadas posibles.

- No es apropiado configurar más de un router de la Intranet con una ruta predeterminada por defecto a menos que dicho router tenga una conexión a Internet a través de un ISP. Si lo hace puede provocar que los routers sin conectividad con destinos desconocidos se envíen paquetes a ellos mismos, con lo que se produce una imposibilidad de acceso. La excepción es aquellos routers que no intercambian la información de enrutamiento dinámico o que tienen solamente conexiones ocasionales con la Intranet a través de medios tales como RDSI o SVC de Frame-Relay.

- Los routers que no intercambian información de enrutamiento dinámico o que se encuentran en conexiones de acceso telefónico, como RDSI o SVC de Frame-Relay, deben configurarse como una ruta predeterminada por defecto.

- Si una Intranet no está conectada a ninguna red externa, como Internet, la configuración de red predeterminada debe colocarse en uno o varios routers que se encuentren en el núcleo de la red y que tengan toda la topología de enrutamiento de red de la Intranet específica.

4.1.4 Configuración de una red de último recurso

El siguiente comando muestra la configuración de una red de por defecto o de último recurso:

```
Router(config)#ip default-network[dirección IP de la red de ultimo
recurso]
```

4.2 ENRUTAMIENTO DINÁMICO

Si se diseñasen redes que utilizaran exclusivamente rutas estáticas sería tedioso administrarlas y no responderían bien a las interrupciones y a los cambios de topología que suelen suceder con cierta frecuencia. Para responder a estos problemas se desarrollaron los protocolos de enrutamiento dinámico.

Los protocolos de enrutamiento dinámico son algoritmos que permiten que los routers publiquen, o anuncien, la existencia de la información de ruta de red IP necesaria para crear la tabla de enrutamiento. Dichos algoritmos también determinan el criterio de selección de la ruta que sigue el paquete cuando se le presenta al router esperando una decisión de conmutar. Los objetivos del protocolo de enrutamiento consisten en proporcionar al usuario la posibilidad de seleccionar la ruta idónea en la red, reaccionar con rapidez a los cambios de la misma y realizar

dichas tareas de la manera más sencilla y con la menor sobrecarga del router posible.

Los protocolos de enrutamiento dinámico se configuran en un router para poder describir y administrar dinámicamente las rutas disponibles en la red.

Para habilitar un protocolo de enrutamiento dinámico, se han de realizar las siguientes tareas:

- Seleccionar un protocolo de enrutamiento.
- Seleccionar las redes IP que serán anunciadas.

También se han de asignar direcciones de red/subred y las máscaras de subred apropiadas a las distintas interfaces. El enrutamiento dinámico utiliza difusiones y multidifusiones para comunicarse con otros routers.

El comando **router** es el encargado de iniciar el proceso de enrutamiento, posteriormente se asocian las redes con el comando **network**.

```
router(config)#router [protocolo] [ID o sistema autónomo]
router(config-router)#network [número de red directamente conectada]
```

4.3 INTRODUCCIÓN A RIP

RIP (Protocolo de información de enrutamiento) es uno de los protocolos de enrutamiento más antiguos utilizado por dispositivos basados en IP. Su implementación original fue para el protocolo Xerox a principios de los ochenta. Ganó popularidad cuando se distribuyó con UNIX como protocolo de enrutamiento para esa implementación TCP/IP. RIP es un protocolo de **vector de distancia** que utiliza la cuenta de **saltos** del router como métrica. La cuenta de saltos máxima de RIP es 15. Cualquier ruta que exceda de los 15 saltos se etiqueta como inalcanzable al establecerse la cuenta de saltos en 16. En RIP la información de enrutamiento se propaga de un router a los otros vecinos por medio de una difusión de IP usando el protocolo UDP y el puerto 520.

El protocolo **RIPv1** (versión 1) es un protocolo de enrutamiento con clase que no admite la publicación de la información de la máscara de red. El protocolo **RIPv2** (versión 2) es un protocolo sin clase que admite CIDR, VLSM, resumen de rutas y seguridad mediante texto simple y autenticación MD5.

4.3.1 Características de RIPv1 y RIPv2

- RIP es un protocolo de enrutamiento basado en vectores distancia.
- RIP utiliza el número de saltos como métrica para la selección de rutas.
- El número máximo de saltos permitido en RIP es 15.
- RIP difunde actualizaciones de enrutamiento por medio de la tabla de enrutamiento completa cada 30 segundos, por omisión.
- RIP puede realizar equilibrado de carga en un máximo de seis rutas de igual coste (la especificación por omisión es de cuatro rutas).
- **RIPv1** requiere que se use una sola máscara de red para cada número de red de clase principal que es anunciado. La máscara es una máscara de subred de longitud fija. El estándar RIP-1 no contempla actualizaciones desencadenadas.
- **RIPv2** permite máscaras de subred de longitud variable (VLSM) en la interconexión. El estándar RIPv2 permite actualizaciones desencadenadas, a diferencia de RIPv1. La definición del número máximo de rutas paralelas permitidas en la tabla de enrutamiento faculta a RIP para llevar a cabo el equilibrado de carga.

4.3.2 Sintaxis de la configuración de RIP

El proceso de configuración de RIP es bastante simple, una vez iniciado el proceso de configuración se deben especificar las redes que participan en el enrutamiento. Si es necesario la versión y el balanceo de ruta.

```
Router(config)#router rip
Router(config-router)#network [dirección de red]
Router(config-router)#version [tipo de versión]
Router(config-router)#maximum-paths [número]
```

Donde:

- **Network**: especifica las redes directamente conectadas al router que serán anunciadas por RIP.
- **Version**: adopta un valor de 1 o 2 para especificar la versión de RIP que se va a utilizar. Si no se especifica la versión, el software IOS adopta

como opción predeterminada el envío de RIP versión 1 pero recibe actualizaciones de ambas versiones, 1 y 2.

- **maximum-paths** (opcional): habilita el equilibrado de carga.

NOTA:

RIP no lleva identificadores de proceso ni de sistema autónomo, por lo tanto no es posible hacer distinciones entre distintos dispositivos.

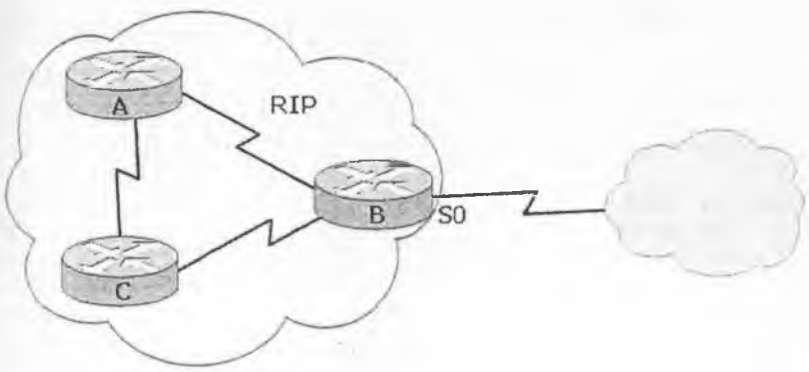
4.3.3 Redistribución estática en RIP

Cuando un sistema autónomo posee una sola puerta de entrada/salida se puede configurar una ruta estática o una ruta estática por defecto de manera que todos los paquetes que quieran llegar a múltiples redes externas lo hagan por medio de esa ruta preestablecida. Para que todos los routers contenidos dentro del mismo sistema autónomo tengan conocimiento de la existencia de esa ruta es necesario redistribuirla dentro del protocolo. Esto se hace con el comando **redistribute static**.

4.4 CASO PRÁCTICO

4.4.1 Configuración de redistribución estática en RIP

En el ejemplo se ha configurado una ruta estática por defecto, que sale a través de la interfaz Serial 0 del router B. Esta interfaz se ha desactivado de manera que no transmita información de protocolo hacia el router D utilizando el comando **passive-interface**.




```
Router(config)#ip route 0.0.0.0 0.0.0.0 serial0
Router(config)#router rip
Router(config-router)#network 192.168.1.0
Router(config-router)#network 200.200.10.0
Router(config-router)#redistribute static
Router(config-router)#passive-interface serial 0
```

La siguiente captura del show ip route del router **A** muestra en la última línea cómo ha aprendido la ruta estática por medio de RIP ilustrado por **R***, donde **R** es RIP y * ruta candidata por defecto.

```
Router_A#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 172.25.1.1 to network 0.0.0.0

C    192.168.1.0/24 is directly connected, Ethernet0
C    200.200.1.0/24 is directly connected, Ethernet1
R    204.170.0.0/24 [120/5] via 172.25.2.1, 00:00:15, Serial0
R    172.16.0.0/16 [120/8] via 172.25.2.1, 00:00:20, Serial1
R*   0.0.0.0/0 [120/1] via 172.25.2.1, 00:00:02, Serial0.1
```

4.5 VERIFICACIÓN DE RIP

El show ip route muestra una tabla de enrutamiento donde se observan dos redes directamente conectadas identificadas con la letra **C**, y dos aprendidas por RIP que llevan la letra **R**.

```
Router#show ip route
Codes: C - connected,S - static,I - IGRP,R - RIP,M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external,O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1,N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * -
candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, Ethernet0
C    200.200.1.0/24 is directly connected, Ethernet1
R    204.170.0.0/24 [120/5] via 172.25.2.1, 00:00:15, Serial0
R    172.16.0.0/16 [120/8] via 172.25.2.1, 00:00:20, Serial1
```

La línea:

```
R    204.170.0.0/24 [120/5] via 172.25.2.1, 00:00:15, Serial0
```

Se interpreta de la siguiente manera:

- **R**: protocolo de enrutamiento, en este caso RIP.
- **204.170.0.0/24**: red aprendida.
- **[120/5]** : distancia administrativa/métrica, en este caso la métrica son saltos.
- **via 172.25.2.1**: camino por el cual se ha aprendido.
- **00:00:15**: tiempo transcurrido desde la última actualización, RIP se actualiza cada 30 segundos.
- **Serial0**: interfaz de salida/entrada.

Para ver los procesos que ejecuta RIP utilice el comando:

```
debug ip rip
```

Copia de un **show ip protocols**:

```
Router#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 7 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 1, receive any version
    Interface         Send  Recv   Key-chain
    Ethernet1         1     1 2
  Routing for Networks:
    162.168.1.0
    200.200.1.0
  Routing Information Sources:
    Gateway         Distance      Last Update
         200.200.1.1          120          00:00:17
       Distance: (default is 120)
```

4.6 INTRODUCCIÓN A IGRP

IGRP (Protocolo de enrutamiento de gateway interior) es un protocolo de vector de distancia mejorado que fue desarrollado por Cisco Systems a mediados de los ochenta. Fue diseñado para corregir algunos de los defectos de RIP y para proporcionar un mejor soporte para redes grandes con enlaces de diferentes anchos de banda. IGRP calcula su métrica en base a diferentes atributos de ruta de red que puede configurar el usuario, como el retraso de red, ancho de banda y el retraso basados en la velocidad y capacidad relativas de la interfaz. Los atributos de carga y fiabilidad se calculan según el rendimiento de la interfaz en la gestión de tráfico real de la red, aunque no están activados de manera predeterminada para las decisiones de enrutamiento.

Como RIP, IGRP utiliza publicaciones IP para comunicar la información de enrutamiento a los routers vecinos. No obstante, IGRP está designado como su propio protocolo de capa de transporte. No depende de UDP o TCP para comunicar la información de la ruta de red. Como IGRP no tiene mecanismos de retroalimentación, funciona de una manera similar a UDP.

IGRP ofrece tres importantes mejoras sobre el protocolo RIP. En primer lugar, la métrica de IGRP puede admitir una red con un número máximo de 255 saltos de router.

En segundo lugar, la métrica de IGRP puede distinguir entre los diferentes tipos de medios de conexión y los costes asociados a cada uno de ellos. En tercer lugar, IGRP ofrece una convergencia de funcionalidad enviando la información sobre cambios en la red a medida que está disponible, en vez de esperar a las horas programadas con regularidad para la actualización.

IGRP es un protocolo de enrutamiento basado en vectores de distancia, sus características son:

- **Escalabilidad mejorada**: enrutamiento en redes más grandes, posee un número máximo predeterminado de 100 saltos, aunque puede ser configurado con hasta 255 saltos.

- **Métrica sofisticada**: métrica compuesta que proporciona una mayor flexibilidad en la selección de rutas. Se usa el retraso de interconexión y el ancho de banda y se pueden incluir otros parámetros como la fiabilidad, la carga y la MTU.

- **Soporte de múltiples rutas**: IGRP puede mantener hasta un máximo de seis rutas de coste diferente entre redes de origen y destino. Se pueden usar varias rutas para aumentar el ancho de banda disponible o para conseguir redundancia de rutas. IGRP permite actualizaciones desencadenadas.

RECUERDE:

El término convergencia hace referencia a la capacidad de los routers de poseer la misma información de enrutamiento actualizada. Las siglas VLSM son las de máscara de subred de longitud variable.

RECUERDE:

Los protocolos vector distancia inundan la red con broadcast de actualizaciones de enrutamiento.

RECUERDE:

Protocolo	RIP	RIPv2	IGRP	EIGRP	IS-IS	OSPF
Vector distancia	X	X	X	X		
Estado de enlace					X	X
Resumen automático de ruta	X	X	X	X	X	
Resumen manual de ruta	X	X	X	X	X	X
Soporte VLSM		X		X	X	X
Propietario de Cisco			X	X		
Convergencia	Lento	Lento	Lento	Muy rápido	Muy rápido	Muy rápido
Distancia administrativa	120	120	100	90	115	110
Tiempo de actualización	30	30	90			
Métrica	Saltos	Saltos	Com-puesta	Com-puesta	Coste	Coste

4.7 FUNDAMENTOS PARA EL EXAMEN

- Recuerde las condiciones necesarias para la utilización de rutas estáticas.
- Analice las diferencias entre las rutas estáticas y las rutas estáticas por defecto y cuáles emplear en cada situación.
- Tenga en cuenta las directrices recomendables a la hora de configurar un enrutamiento estático.

- Estudie el funcionamiento de RIPv1 y RIPv2, compárelos entre ambos y con otros protocolos de enrutamiento vector distancia.
- Memorice todos los comandos necesarios para la activación de RIPv1 y RIPv2 y su verificación.
- Ejercite todas las configuraciones en dispositivos reales o en simuladores.

Capítulo 5

ENRUTAMIENTO AVANZADO

5.1 INTRODUCCIÓN A EIGRP

El protocolo de enrutamiento de gateway interior mejorado **EIGRP** (*Enchaced Interior Gateway Routing Protocol*) es una versión mejorada del protocolo IGRP original desarrollado por Cisco Systems.

EIGRP mantiene el mismo algoritmo de **vector de distancia** y la información de métrica original de IGRP; no obstante, se han mejorado apreciablemente el tiempo de convergencia y los aspectos relativos a la capacidad de ampliación. EIGRP e IGRP usan cálculos de métrica diferentes. EIGRP multiplica la métrica de IGRP por un factor de 256. Esto ocurre porque EIGRP usa una métrica que tiene 32 bits de largo, e IGRP usa una métrica de 24 bits. La información EIGRP puede multiplicarse o dividirse por 256 para un intercambio fácil con IGRP. IGRP tiene un número de saltos máximo de 255. El límite máximo para el número de saltos en EIGRP es 224. Esto es más que suficiente para admitir grandes redes.

EIGRP ofrece características que no se encontraban en su antecesor, IGRP como el soporte para **VLSM** y los resúmenes de ruta. Además, EIGRP ofrece características que se encuentran en protocolos como OSPF, como las actualizaciones incrementales parciales y un tiempo de convergencia reducido. Como en el caso del protocolo IGRP, EIGRP publica la información de la tabla de enrutamiento solo a los routers vecinos.

EIGRP mantiene las siguientes tres tablas:

- Tabla de vecinos.
- Tabla de topología.
- Tabla de enrutamiento.

Los routers vecinos se descubren por medio de un protocolo **Hello** sencillo intercambiado por los routers que pertenecen a la misma red física estableciendo adyacencias. Hello utiliza para intercambiar paquetes de saludo una dirección multicast **224.0.0.10**. Una vez descubiertos los routers vecinos, EIGRP utiliza un protocolo de transporte fiable para garantizar la entrega correcta y ordenada de la información y las actualizaciones de la tabla de enrutamiento. Un router hace el seguimiento de sus propias rutas conectadas y, además, de todas las rutas públicas de los routers vecinos. Basándose en esta información, EIGRP puede seleccionar eficaz y rápidamente la ruta de menor coste hasta un destino y garantizar que la ruta no forma parte de un bucle de enrutamiento; esta ruta elegida como principal será la llamada **Sucesor**.

Al almacenar la información de enrutamiento de los routers vecinos, el algoritmo puede determinar con mayor rapidez una ruta de sustitución o un **sucesor factible** en caso de que haya un fallo de enlace o cualquier otro evento de modificación de la topología.

El saludo y la información de enrutamiento EIGRP son transportados mediante el protocolo de transporte EIGRP. El transporte EIGRP define un protocolo fiable de publicación, acuse de recibo y petición para garantizar que el saludo y la información de enrutamiento se distribuyen adecuadamente a todos los routers vecinos.

Cuando existen cambios de topologías EIGRP recurre a **DUAL** (algoritmo de actualización difusa) para conseguir una rápida convergencia entre los routers, estos almacenan sus propias tablas de enrutamiento con rutas alternativas (sucesor factible), si no existiera alguna ruta alternativa, EIGRP recurre a sus routers vecinos para conseguir información acerca de ese camino alternativo.

NOTA:

EIGRP combina las ventajas de los protocolos de estado de enlace con las de los protocolos de vector de distancia.

5.1.1 Métricas EIGRP

EIGRP utiliza una métrica de enrutamiento compuesta. La ruta que posea la métrica más baja será considerada la ruta óptima. Las métricas de EIGRP están ponderadas mediante constantes desde K0 hasta K5 que convierten los vectores de métrica EIGRP en cantidades escalables.

La métrica utilizada por EIGRP se compone de:

- **K1=Ancho de banda**: valor mínimo de ancho de banda en kbps en la ruta hacia el destino.
- **K2=Fiabilidad**: fiabilidad entre el origen y el destino, determinado por el intercambio de mensajes de actividad expresado en porcentajes.
- **K3=Retraso**: retraso de interfaz acumulado a lo largo de la ruta en microsegundos.
- **K4=Carga**: carga de un enlace entre el origen y el destino. Medido en bits por segundo es el ancho de banda real de la ruta.
- **K5=MTU**: valor de la unidad máxima de transmisión de la ruta expresado en bytes.

La métrica EIGRP se calcula en base a las variables resultantes de las constantes K1 y K3. El valor mínimo de ancho de banda se divide por 107 multiplicado por 256, mientras que el retraso es la sumatoria de todos los retrasos de la ruta en microsegundos multiplicado por 256.

NOTA:

La información de MTU se envía en los mensajes de actualización del protocolo, sin embargo no se utiliza en el cálculo de la métrica.

5.2 CONFIGURACIÓN DE EIGRP

En el proceso de configuración de EIGRP se debe especificar el número de **sistema autónomo** (AS) que identificará al conjunto de routers que participan de ese mismo protocolo, posteriormente asociar las redes o subredes directamente conectadas, y los parámetros opcionales si así se requiriera.

```
router(config)#router eigrp [sistema autónomo]
router(config-router)#network [dirección de red]
router(config-router)#eigrp log-neighbor-changes
Router(config)#interface [tipo][número]
router(config-if)#bandwidth [kilobits]
```

En versiones actuales de IOS se puede especificar una wildcard de tal manera que identifique si se trata de una red o subred la que deba anunciarse. En capítulos posteriores se explica el funcionamiento detallado de las wildcard.

```
router(config)#router eigrp [sistema autónomo]
router(config-router)#network [dirección de red][wildcard]
```

Donde:

- **router eigrp**: especifica como protocolo de enrutamiento a EIGRP para un sistema autónomo, este valor varía de 1 a 65535.
- **network**: especifica las redes directamente conectadas al router que serán anunciadas por EIGRP.
- **bandwidth**: el proceso de enrutamiento utiliza el comando bandwidth para calcular la métrica y es conveniente configurar el comando para que coincida con la velocidad de línea de la interfaz.
- **log-neighbor-changes**: habilita el registro de los cambios de adyacencia de vecinos para monitorear la estabilidad del sistema de enrutamiento y para ayudar a detectar problemas.

Para el caso que desee desactivar el resumen de ruta, por ejemplo al tener redes discontinuas, puede ejecutar el comando:

```
router(config-router)#no auto-summary
```

Para crear manualmente un resumen de ruta puede hacerlo indicando el AS (sistema autónomo EIGRP) y la red de resumen:

```
router(config-router)#ip summary-address eigrp [sistema autónomo]
[dirección de red-máscara]
```

NOTA:

EIGRP se redistribuye automáticamente con otros sistemas autónomos EIGRP identificando las rutas como EIGRP externo y con IGRP si es el mismo número de sistema autónomo.

5.2.1 Equilibrado de carga

El equilibrado de carga en los routers con rutas de coste equivalente suele ser por defecto de un máximo de cuatro. El equilibrado puede modificarse hasta un máximo de seis rutas. EIGRP puede a su vez equilibrar tráfico por múltiples rutas con diferentes métricas utilizando un multiplicador de varianza, por defecto el valor de la varianza es uno equilibrando la carga por costes equivalentes.

```
router(config)#router eigrp [sistema autónomo]
router(config-router)#network [dirección de red]
Router(config-router)#maximum-paths [número máximo]
Router(config-router)#variance [métrica] [multiplicador]
```

5.2.2 Ajustes de los temporizadores

Los intervalos de hello y hold por defecto mantienen los valores de 5 y 15 segundos respectivamente. Estos valores pueden modificarse dentro de las respectivas interfaces teniendo en cuenta que deben ser iguales para todos los routers del sistema autónomo.

```
Router(config-if)#ip hello-interval eigrp[sistema autónomo]
[segundos]
Router(config-if)#ip hold-time eigrp [sistema autónomo] [segundos]
```

5.2.3 Filtrados de rutas

EIGRP permite el filtrado de rutas en las interfaces de manera entrante o saliente asociando listas de acceso al protocolo.

```
Router(config)#router eigrp [sistema autónomo]
Router(config-router)#distribute-list[número de lista][in|out]
[interfaz]
```

5.2.4 Desactivación de una interfaz EIGRP

Para impedir que una interfaz envíe publicaciones de enrutamiento EIGRP se puede desactivar la interfaz dentro del protocolo especificando el tipo y número de dicha interfaz.

```
Router(config)#router eigrp [sistema autónomo]
Router(config-router)#passive-interface [tipo][número]
```

5.2.5 Redistribución estática en EIGRP

EIGRP redistribuye rutas aprendidas estáticamente dirigidas hacia un destino en particular o por defecto.

```
Router(config)#ip route [red destino][gateway|interfaz]
Router(config)#router eigrp [sistema autónomo]
Router(config-router)#redistribute static
```

5.2.6 Configuración de intervalos hello

Los intervalos de saludo y los tiempos de espera se configuran por interfaz y no tienen que coincidir con otros routers EIGRP para establecer adyacencias.

```
Router(config-if)#ip hello-interval eigrp [número de AS][segundos]
```

Si cambia el intervalo de saludo, asegúrese de cambiar también el tiempo de espera a un valor igual o superior al intervalo de saludo. De lo contrario, la adyacencia de vecinos se desactivará después de que haya terminado el tiempo de espera y antes del próximo intervalo de saludo.

```
Router(config-if)#ip hold-time eigrp [número de AS][segundos]
```

El valor segundos para los intervalos de saludo y de tiempo de espera puede variar de 1 a 65535.

5.3 AUTENTICACIÓN EIGRP

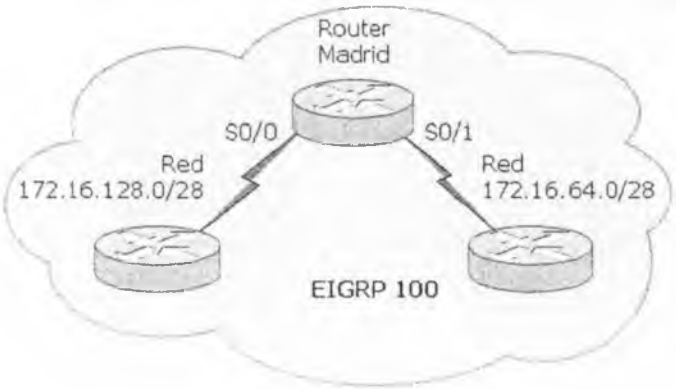
La autenticación EIGRP comienza creando una cadena de claves, numerarla y asociarla con la clave correspondiente. Posteriormente se puede configurar un sistema seguro de encriptación como MD5 dentro de la interfaz y habilitar la autenticación dentro de la misma interfaz.

```
Router(config)#key chain nombre
Router(config-keychain)#key número
Router(config-keychain-key)#key-string nombre
Router(config-keychain-key)#exit
Router(config-keychain)#exit
Router(config)#interface [tipo][número]
Router(config-if)#ip authentication mode eigrp [sistema autónomo]
md5
Router(config-if)#ip authentication key-chain eigrp [sistema
autónomo] nombre de la cadena
```

5.4 CASO PRÁCTICO

5.4.1 Configuración de un AS con EIGRP

La sintaxis muestra la configuración de un sistema autónomo 100 con EIGRP.




```
Madrid(config)#router eigrp 100
Madrid(config-router)#network 172.16.128.0 0.0.15.255
Madrid(config-router)#network  172.16.64.0 0.0.15.255
Madrid(config-router)#eigrp log-neighbor-changes
Madrid(config)#interface serial 0/0
Madrid(config-if)#ip address 172.16.128.1 255.255.240.0
```

```
Madrid(config-if)#bandwidth 64
Madrid(config-if)#clock rate 200000
Madrid(config-if)#no shutdown
Madrid(config)#interface serial 0/1
Madrid(config-if)#ip address 172.16.64.1 255.255.240.0
Madrid(config-if)#bandwidth 64
Madrid(config-if)#nc shutdown
```

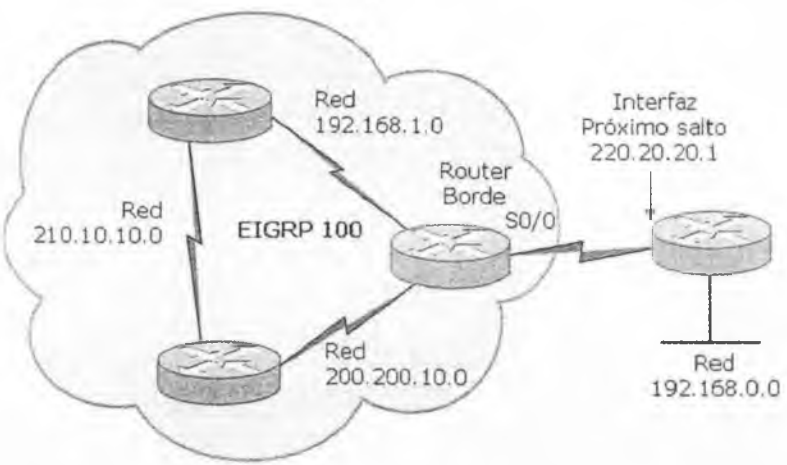
5.4.2 Configuración de filtro de ruta EIGRP

En el ejemplo que sigue se han creado dos listas de acceso estándar, la ACL 10 denegará cualquier información de enrutamiento de la red 192.168.20.0, mientras que la ACL 20 enviará información de enrutamiento EIGRP de la red 200.20.20.0. Ambas listas se asocian al protocolo de enrutamiento EIGRP 100.

```
Router#configure terminal
Router(config)#access-list 10 deny 192.168.50.0 0.0.0.255
Router(config)#access-list 10 permit any
Router(config)#access-list 20 permit 200.20.20.0 0.0.0.255
Router(config)#router eigrp 100
Router(config-router)#distribute-list 10 in Serial 0/0
Router(config-router)#distribute-list 20 out Serial 0/1
Router(config-router)#network 172.16.0.0
Router(config-router)#network 192.168.10.0
```

5.4.3 Configuración de redistribución estática en EIGRP

En el ejemplo se ilustra un router como única salida y entrada para el sistema autónomo 100. La distribución estática permite que todos los routers implicados en el mismo sistema conozcan la ruta estática como salida predeterminada.



```
Borde(config)#ip route 192.168.0.0 255.255.255.0 220.20.20.1 120

Borde(config)#router eigrp 100
Borde(config-router)#network 192.168.1.0
Borde(config-router)#network 200.200.10.0
Borde(config-router)#redistribute static
Borde(config-router)#passive-interface serial 0
```

5.5 VERIFICACIÓN EIGRP

Algunos comandos para la verificación y control EIGRP son:

- **show ip route**: muestra la tabla de enrutamiento.
- **show ip protocols**: muestra los parámetros todos los protocolos.
- **show ip eigrp neighbors**: muestra la información de los vecinos EIGRP.
- **show ip eigrp topology**: muestra la tabla de topología EIGRP.
- **debug ip eigrp**: muestra la información de los paquetes.

```
Router#show ip protocols
Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 55
  Automatic network summarization is in effect
  Automatic address summarization:
    192.168.20.0/24 for Loopback0, Serial0
    192.170.0.0/16 for Ethernet0
      Summarizing with metric 128256
  Maximum path: 4
  Routing for Networks:
    172.30.0.0
    192.168.20.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.25.5.1            90      00:01:49
  Distance: internal 90 external 170
```

```
Router#show ip route eigrp
D    172.22.0.0/16 [90/2172416] via 172.25.2.1, 00:00:35, Serial0.1
     172.25.0.0/16 is variably subnetted, 6 subnets, 4 masks
D    172.25.25.6/32 [90/2300416] via 172.25.2.1, 00:00:35, Serial0.1
D    172.25.25.1/32 [90/2297856] via 172.25.2.1, 00:00:35, Serial0.1
D    172.25.1.0/24 [90/2172416] via 172.25.2.1, 00:00:35, Serial0.1
D    172.25.0.0/16 is a summary, 00:03:10, Null0
D    10.0.0.0/8 [90/4357120] via 172.25.2.1, 00:00:35, Serial0.1
```

*Observe la métrica en [90/**4357120**]

*Distancia administrativa en [**90**/4357120]

5.6 INTRODUCCIÓN A OSPF

El protocolo **OSPF,** Primero la ruta libre más corta (*Open Shortest Path First*) fue creado a finales de los ochenta. Se diseñó para cubrir las necesidades de las grandes redes IP que otros protocolos como RIP no podían soportar, incluyendo VLSM, autenticación de origen de ruta, convergencia rápida, etiquetado de rutas conocidas mediante protocolos de enrutamiento externo y publicaciones de ruta de multidifusión. El protocolo OSPF versión 2 es la implementación más actualizada, aparece especificado en la RFC 2328.

OSPF funciona dividiendo una Intranet o un sistema autónomo en unidades jerárquicas de menor tamaño. Cada una de estas áreas se enlaza a un área backbone mediante un router fronterizo. Todos los paquetes enviados desde una dirección de una estación de trabajo de un área a otra de un área diferente atraviesan el área backbone, independientemente de la existencia de una conexión directa entre las dos áreas. Aunque es posible el funcionamiento de una red OSPF únicamente con el área backbone, OSPF escala bien cuando la red se subdivide en un número de áreas más pequeñas.

OSPF es un protocolo de enrutamiento por estado de enlace que a diferencia de RIP e IGRP que publican sus rutas solo a routers vecinos, los routers OSPF envían publicaciones del estado de enlace **LSA** (*Link-State Advertisment*) a todos los routers pertenecientes a la misma área jerárquica mediante una multidifusión de IP. La LSA contiene información sobre las interfaces conectadas, la métrica utilizada y otros datos adicionales necesarios para calcular las bases de datos de la ruta y la topología de red. Los routers OSPF acumulan información sobre el estado de enlace y ejecutan el algoritmo **SPF** (que también se conoce con el nombre de su creador, Dijkstra) para calcular la ruta más corta a cada nodo.

Para determinar qué interfaces reciben las publicaciones de estado de enlace, los routers ejecutan el protocolo OSPF **Hello**. Los routers vecinos intercambian mensajes hello para determinar qué otros routers existen en una determinada interfaz y sirven como mensajes de actividad que indican la accesibilidad de dichos routers.

Cuando se detecta un router vecino, se intercambia información de topología OSPF. Cuando los routers están sincronizados, se dice que han formado una adyacencia.

Las LSA se envían y reciben solo en adyacencias. La información de la LSA se transporta en paquetes mediante la capa de transporte OSPF que define un proceso fiable de publicación, acuse de recibo y petición para garantizar que la información de la LSA se distribuye adecuadamente a todos los routers de un área. Existen cuatro tipos de LSA. Los tipos más comunes son los que publican información sobre los enlaces de red conectados de un router y los que publican las redes disponibles fuera de las áreas OSPF.

La métrica de enrutamiento de OSPF es el **coste** que se calcula en base al ancho de banda de la interfaz y es configurable por parte del usuario.

La fórmula para calcular el coste es:

$$\frac{10^8}{\textbf{Ancho de banda}}$$

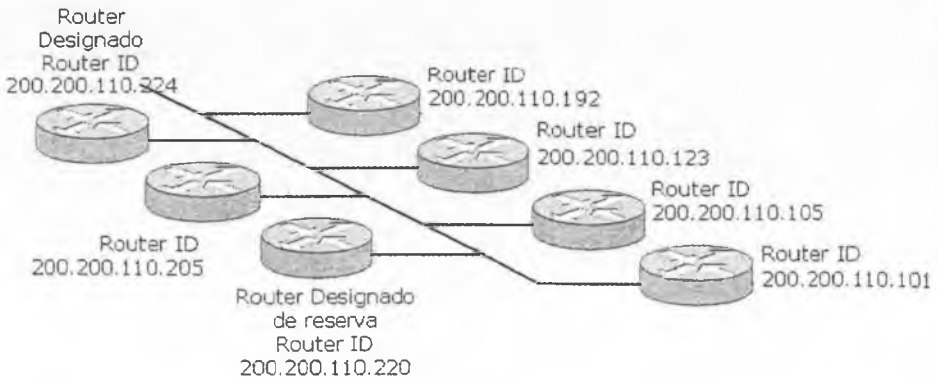
5.6.1 OSPF en una topología multiacceso con difusión

Dado que el enrutamiento OSPF depende del estado de enlace entre dos routers, los vecinos deben reconocerse entre sí para compartir información. Este proceso se hace por medio del protocolo **Hello**.

Los paquetes se envían cada 10 segundos (forma predeterminada) utilizando la dirección de multidifusión 224.0.0.5. Para declarar a un vecino caído el router espera cuatro veces el tiempo del intervalo **Hello** (intervalo **Dead**).

Los routers de un entorno multiacceso, como un entorno Ethernet, deben elegir un router designado (**DR**) y un router designado de reserva (**BDR**) para que representen a la red.

Un DR lleva a cabo tareas de envío y sincronización. El **BDR** solo actuará si el **DR** falla. Cada router debe establecer una adyacencia con el DR y el BDR.



En redes con difusión se lleva a cabo la elección de DR y BDR

NOTA:

Un router se ve a sí mismo listado en un paquete Hello que recibe de un vecino.

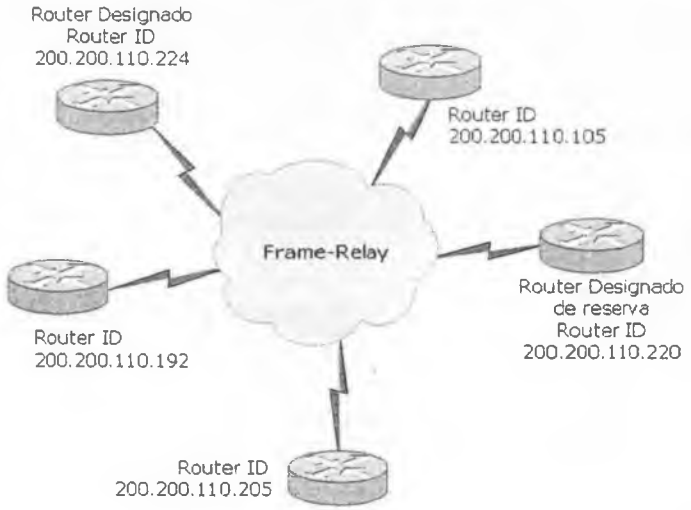
5.6.2 Elección del router designado

La elección de un router designado (DR) y un router designado de reserva (BDR) en una topología multiacceso con difusión cumple los siguientes requisitos:

- El router con el valor de prioridad más alto es el router designado **DR**.
- El router con el segundo valor es el router designado de reserva **BDR**.
- El valor predeterminado de la prioridad OSPF de la interfaz es **1**. Un router con prioridad 0 no es elegible. En caso de empate se usa el ID de router.
- ID de router. Este número de 32 bits identifica únicamente al router dentro de un sistema autónomo. La dirección IP más alta de una interfaz activa se elige por defecto.

5.6.3 OSPF en una topología NBMA

Las redes **NBMA** son aquellas que soportan más de dos routers pero que no tienen capacidad de difusión. Frame-Relay, ATM, X.25 son algunos ejemplos de redes NBMA. La selección del DR se convierte en un tema importante ya que el DR y el BDR deben tener conectividad física total con todos los routers de la red.



OSPF en redes NBM: debe existir conectividad entre todos los routers

5.6.4 OSPF en una topología punto a punto

En redes punto a punto el router detecta dinámicamente a sus vecinos enviando paquetes Hello con la dirección de multidifusión 224.0.0.5. **No se lleva a cabo elección y no existe concepto de DR o BDR.**

Los intervalos Hello y Dead son de 10 y 40 segundos respectivamente.

OSPF en redes punto a punto:
no hay elección de DR ni BDR.

5.6.5 Mantenimiento de la información de enrutamiento

Paso 1 - Un router advierte un cambio de estado de un enlace y hace una multidifusión de un paquete **LSU** (actualización de estado de enlace) con la IP **224.0.0.6**.

Paso 2 - El DR acusa recepción e inunda la red con la LSU utilizando la dirección de multidifusión 224.0.0.5.

Paso 3 - Si se conecta un router con otra red, reenviará la LSU al DR de dicha red.

Paso 4 - Cuando un router recibe la LSU que incluye la LSA (publicación de estado de enlace) diferente, cambiará su base de datos.

5.7 CONFIGURACIÓN DE OSPF EN UNA SOLA ÁREA

Habilitar OSPF por medio del comando:

```
Router(config)#router ospf número de proceso
Router(config-router)#network dirección wildcard area área
```

Donde:

- **Número de proceso**: es el número que se usa internamente para identificar si existen múltiples procesos OSPF en ejecución dentro del router.
- **Network**: identifica las redes directamente conectadas, identificadas por medio de su correspondiente máscara de wildcard.
- **Area**: para cada red, deberá identificar además a qué área pertenece. El área principal o de Backbone es el área 0.

5.7.1 Administración de la selección del DR y BDR

La elección del DR y del DBR puede manipularse acorde a las necesidades existentes variando los valores de la prioridad dentro de la interfaz o subinterfaz que participe en el dominio OSPF (rango de 1 a 65535).

```
Router#configure terminal
Router(config)#interface [tipo][número]
Router(config-if)#ip ospf priority [1-65535]
```

Esta decisión puede aplicarse también con la creación de una interfaz de Loopback cuyo valor se tendrá en cuenta como prioritario al momento de definir el ID del router.

```
Router(config)#interface loopback[número]
Router(config-if)#ip address [dirección IP-máscara]
```

RECUERDE:

Para la configuración de OSPF, las interfaces que participan del proceso deben estar configuradas y activas previamente.

5.7.2 Cálculo del coste del enlace

El coste se calcula usando la fórmula 108/bandwidth, donde el ancho de banda se expresa en bps. El Cisco IOS determina automáticamente el coste basándose en el ancho de banda de la interfaz.

Para modificar el ancho de banda sobre la interfaz utilice el siguiente comando:

```
Router(config)#interface serial 0/0
Router(config-if)#bandwidth 64
```

Use el siguiente comando de configuración de interfaz para cambiar el coste del enlace:

```
Router(config-if)#ip ospf cost number
```

5.7.3 Autenticación OSPF

Para crear una contraseña de autenticación en texto simple utilice el siguiente comando dentro de la interfaz:

```
Router(config-if)#ip ospf authentication-key contraseña
```

Para establecer un nivel de encriptación en la contraseña de autenticación puede utilizarse el siguiente comando dentro de la interfaz:

```
Router(config-if)#ip ospf message-digest-key [identificador] md5
[tipo de encriptación]
```

```
Router(config)#router ospf [número de proceso]
Router(config-router)#area [número] authentication
Router(config-router)#area [número] authentication message-digest
```

5.7.4 Administración del protocolo Hello

De manera predeterminada, los paquetes de saludo OSPF (Hello) se envían cada 10 segundos en segmentos multiacceso y punto a punto, y cada 30 segundos en segmentos multiacceso sin broadcast (NBMA).

El intervalo muerto (Dead) es el período, expresado en segundos, que el router esperará para recibir un paquete de saludo antes de declarar al vecino desactivado. Cisco utiliza de forma predeterminada cuatro veces el intervalo de Hello. En el caso de los segmentos multiacceso y punto a punto, dicho período es de 40 segundos. En el caso de las redes NBMA, el intervalo muerto es de 120 segundos.

Para configurar los intervalos de Hello y de Dead en una interfaz se deben utilizar los siguientes comandos:

```
Router(config-if)#ip ospf hello-interval [segundos]
Router(config-if)#ip ospf dead-interval [segundos]
```

5.8 OSPF EN MÚLTIPLES ÁREAS

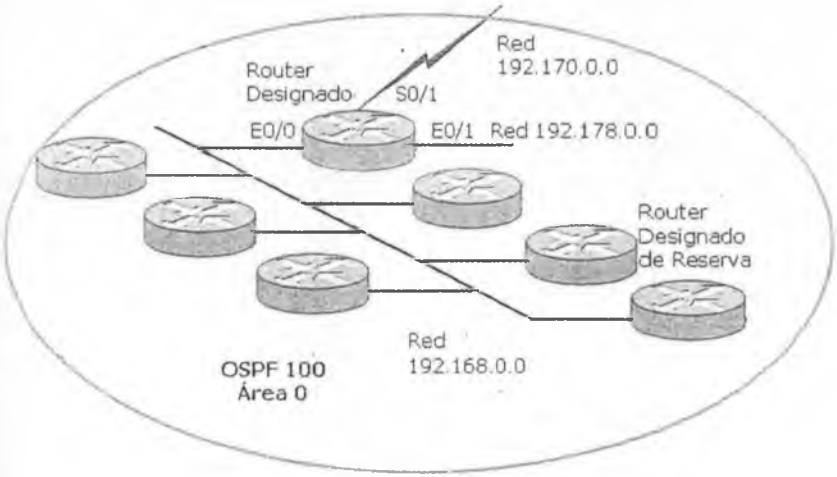
La capacidad de OSPF de separar una gran red en diferentes áreas más pequeñas se denomina enrutamiento jerárquico. Esta red jerárquica permite dividir un **AS** (sistema autónomo) en redes más pequeñas llamadas áreas que se conectan al área 0 o **área de backbone**. Las actualizaciones de enrutamiento interno como el recálculo de la base de datos se producen dentro de cada área, es decir que si por ejemplo una interfaz se torna inestable el recálculo se circunscribe a su área sin afectar al resto. Esta tarea hace que los cálculos **SPF** solo incluyan al área en cuestión sin que esto afecte a las demás áreas.

Las actualizaciones de estado de enlace **LSU** pueden publicar rutas resumidas entre áreas en lugar de una por red. La información de enrutamiento entre áreas puede ser filtrada haciendo más selectivo y eficaz el enrutamiento dinámico.

5.9 CASO PRÁCTICO

5.9.1 Configuración de OSPF en una sola área

En el ejemplo se muestra la sintaxis de la configuración de **OSPF 100** en un router (RouterDR).



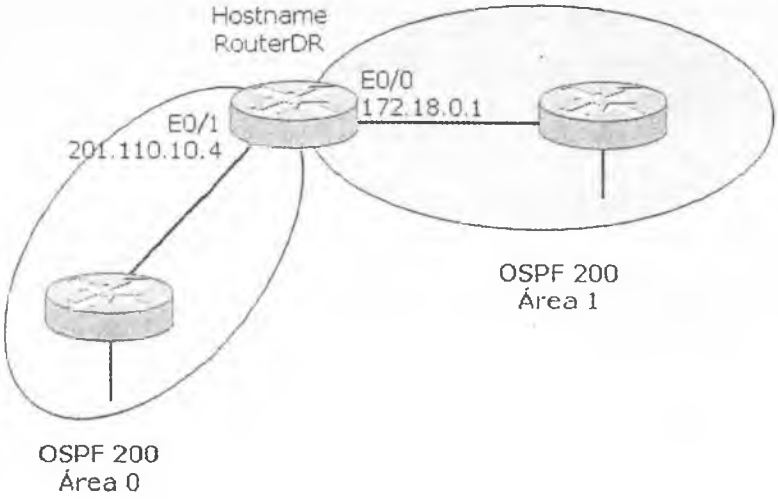

```
RouterDR(config)#router ospf 100
RouterDR(config-router)#network 192.168.0.0 0.0.0.255 area 0
RouterDR(config-router)#network 192.170.0.0 0.0.0.255 area 0
RouterDR(config-router)#network 192.178.0.0 0.0.0.255 area 0
RouterDR(config-if)#exit
RouterDR(config)#interface loopback 1
RouterDR(config-if)#ip address 200.200.10.10 255.255.255.0
RouterDR(config-if)#exit
RouterDR(config)#interface ethernet 0/0
RouterDR(config-if)#ip address 192.168.0.2 255.255.255.0
RouterDR(config-if)#no shutdown
RouterDR(config-if)#ip ospf priority 2
RouterDR(config-if)#bandwidth 64
RouterDR(config-if)#ip ospf cost 10
RouterDR(config-if)#ip ospf message-digest-key 1 md5 AlaKran
RouterDR(config-if)#ip ospf hello-interval 20

RouterDR(config-if)#ip ospf dead-interval 50

RouterDR(config-if)#exit
RouterDR(config)#router ospf 100
RouterDR(config-router)#area 0 authentication
RouterDR(config-router)#area 0 authentication message-digest
```

5.9.2 Configuración de OSPF en múltiples áreas

La sintaxis muestra la configuración básica de OSPF 200 en dos áreas.




```
RouterDR(config)#interface ethernet 0/0
RouterDR(config-if)#ip address 172.18.0.1 255.255.0.0
RouterDR(config-if)#no shutdown
RouterDR(config)#interface ethernet 0/1
RouterDR(config-if)#ip address 201.110.10.4 255.255.255.0
RouterDR(config-if)#no shutdown
RouterDR(config)#router ospf 200
RouterDR(config-router)#network 201.110.10.4 0.0.0.255 area 0
RouterDR(config-router)#network 172.18.0.0 0.0.255.255 area 1
RouterDR(config-if)#exit
```

RECUERDE:

En principio, el router intentará utilizar un ID buscando interfaces virtuales o loopback, si no encuentra configuración de las mismas lo hará con la interfaz física con la dirección IP más alta.

Los valores de los intervalos de Hello y de Dead deben coincidir en los router adyacentes para que OSPF funcione correctamente.

Ante la posibilidad de flapping los routers esperan unos instantes antes de recalcular su tabla de enrutamiento.

5.10 VERIFICACIÓN OSPF

Algunos comandos para la verificación y control OSPF son:

- **show ip route**: muestra la tabla de enrutamiento.
- **show ip protocols**: muestra los parámetros del protocolo.
- **show ip ospf neighbors**: muestra la información de los vecinos OSPF.
- **debug ip ospf events**: muestra adyacencias, DR, inundaciones, etc.
- **debug ip ospf packet**: muestra la información de los paquetes.
- **debug ip ospf hello**: muestra las actualizaciones Hello.

```
Router#show ip protocols

Routing Protocol is "ospf 100"

  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 200.200.10.10
  It is an area border and autonomous system boundary router
  Redistributing External Routes from,
  Number of areas in this router is 3. 3 normal 0 stub 0 nssa
  Maximum path: 4

  Routing for Networks:
    192.168.0.0  0.0.0.255 area 0
    192.170.0.0  0.0.0.255 area 0
    192.178.0.0  0.0.0.255 area 0

  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.0.1          110      00:01:30
    192.170.0.26         110      16:44:07
    122.178.0.1           110      00:01:30

  Distance: (default is 110)
```

5.11 FUNDAMENTOS PARA EL EXAMEN

- Recuerde los conceptos fundamentales sobre el tipo de protocolo que es EIGRP, su funcionamiento, tipos de tablas que utiliza y topologías.
- Analice el funcionamiento de DUAL y cómo descubre las rutas.
- Estudie las métricas utilizadas por EIGRP, cuáles son las constantes y cómo funcionan y las que lo hacen por defecto.
- Estudie todos los comandos completos utilizados para la configuración de EIGRP, incluidos los de verificación de funcionamiento.
- Memorice los conceptos fundamentales sobre el tipo de protocolo que es OSPF, su funcionamiento y los tipos de tablas que utiliza.
- Recuerde las diferentes topologías sobre las que puede funcionar OSPF, en qué caso existe elección de DR y BDR y cómo se hace tal elección.
- Analice la métrica y elección de ruta de OSPF.
- Estudie todos los comandos completos utilizados para la configuración de OSPF, incluidos los de verificación de funcionamiento.
- Tenga un concepto claro del funcionamiento de OSPF en múltiples áreas.
- Ejercite todas las configuraciones en dispositivos reales o en simuladores.

Capítulo 6

REDES INÁLAMBRICAS

6.1 CONCEPTOS BÁSICOS SOBRE WLAN

La utilización de las **WLAN** (Wireless LAN) es hoy en día de uso frecuente y cada vez más veloz, eficaz y seguro. El funcionamiento de las WLAN es similar en muchos aspectos al de las LAN tradicionales. La norma IEEE 802.3 establece el estándar para las redes LAN mientras que el IEEE 802.11 lo hace para la familia de redes inalámbricas. Ambas definen, entre otras cosas, el formato de la trama que se diferencia en que las WLAN no usan una trama estándar 802.3. Por lo tanto, el término Ethernet inalámbrica puede resultar engañoso al ser básicamente diferentes. En el caso de las direcciones MAC es de 6 Bytes (48 bits) para los dos tipos de estándares. La diferencia más grande entre los dos métodos es la posibilidad de transmitir datos sin necesidad de cableado, aunque esto puede estar limitado al espacio aéreo si existen objetos que puedan interferir con las ondas de radiofrecuencia.

Ethernet puede transmitir de forma full-duplex simplemente si un ordenador se encuentra directamente conectado a un puerto de un switch, creando así su propio dominio de colisión. Sin embargo, como se detalló en capítulos anteriores, si el medio es compartido, Ethernet posee herramientas para detectar colisiones y elaborar mecanismos para solucionar tal efecto perjudicial. El **CSMA/CD** permite a los dispositivos escuchar antes de transmitir o generar un algoritmo de espera ante colisiones en el medio compartido. Debido a que la radiofrecuencia (RF) es un medio compartido, se pueden producir colisiones de la misma manera que se producen en un medio compartido cableado. La principal diferencia es que no existe un método por el que un nodo origen pueda detectar que

ha ocurrido una colisión. Por eso, las WLAN utilizan Acceso Múltiple con Detección de Portadora/Carrier y Prevención de Colisiones (**CSMA/CA**) similar en su funcionamiento al CSMA/CD de Ethernet.

La finalidad de este libro no es profundizar más allá de los conceptos básicos, estándares y métodos de seguridad.

6.2 ESTÁNDARES WLAN

El estándar **IEEE 802.11** es un protocolo de comunicaciones que define el uso de las dos capas inferiores del modelo OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento para una red inalámbrica (WLAN). La tecnología clave que contiene el estándar 802.11 es el Espectro de Dispersión de Secuencia Directa (DSSS). El **DSSS** se aplica a los dispositivos inalámbricos que operan dentro de un intervalo de 1 a 2 Mbps. Un sistema de DSSS puede transmitir hasta 11 Mbps, pero si opera por encima de los 2 Mbps se considera que no cumple con la norma.

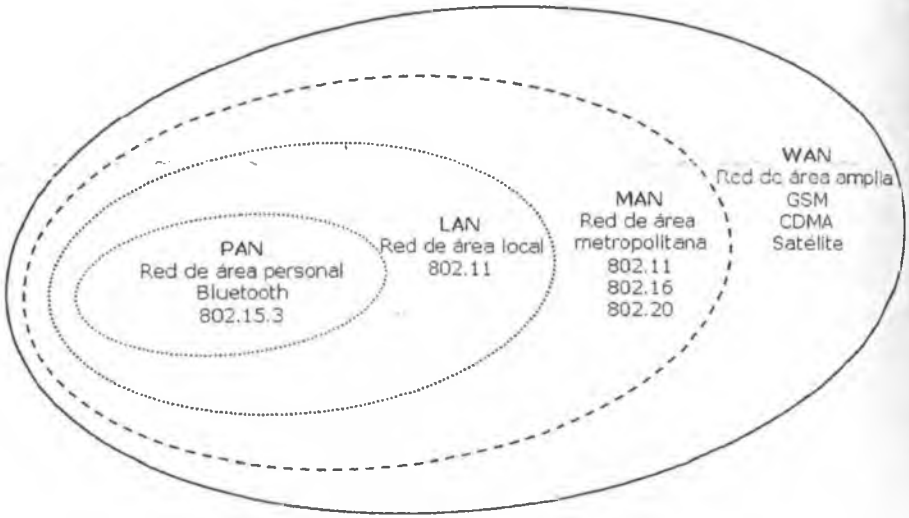


Imagen típica de las WLAN en cada tipo de red y sus tecnologías

6.2.1 802.11b

802.11b también recibe el nombre de Wi-Fi o inalámbrico de alta velocidad y se refiere a los sistemas DSSS que operan a 1, 2; 5,5 y 11 Mbps. Todos

los sistemas 802.11b cumplen con la norma de forma retrospectiva, ya que también son compatibles con 802.11 para velocidades de transmisión de datos de 1 y 2 Mbps solo para DSSS. Esta compatibilidad retrospectiva es de suma importancia ya que permite la actualización de la red inalámbrica sin reemplazar las NIC o los puntos de acceso.

Los dispositivos de 802.11b logran un mayor índice de tasa de transferencia de datos ya que utilizan una técnica de codificación diferente a la del 802.11, permitiendo la transferencia de una mayor cantidad de datos en la misma cantidad de tiempo. La mayoría de los dispositivos 802.11b todavía no alcanzan tasa de transferencia de **11 Mbps** y, por lo general, trabajan en un intervalo de 2 a 4 Mbps.

6.2.2 802.11a

802.11a abarca los dispositivos WLAN que operan en la banda de transmisión de 5 GHz. El uso del rango de 5 GHz no permite la interoperabilidad de los dispositivos 802.11b ya que estos operan dentro de los 2,4 GHz. 802.11a puede proporcionar una tasa de transferencia de datos de 54 Mbps y con una tecnología propietaria que se conoce como duplicación de la velocidad ha alcanzado los **108 Mbps**. En las redes de producción, la velocidad estándar es de 20-26 Mbps.

6.2.3 802.11g

802.11g ofrece tasa de transferencia igual que 802.11a pero con compatibilidad retrospectiva para los dispositivos 802.11b utilizando tecnología de modulación por Multiplexión por División de Frecuencia Ortogonal (OFDM). Cisco ha desarrollado un punto de acceso que permite que los dispositivos 802.11b y 802.11a coexistan en la misma WLAN. El punto de acceso brinda servicios de gateway que permiten que estos dispositivos, que de otra manera serían incompatibles, se comuniquen.

6.2.4 802.11n

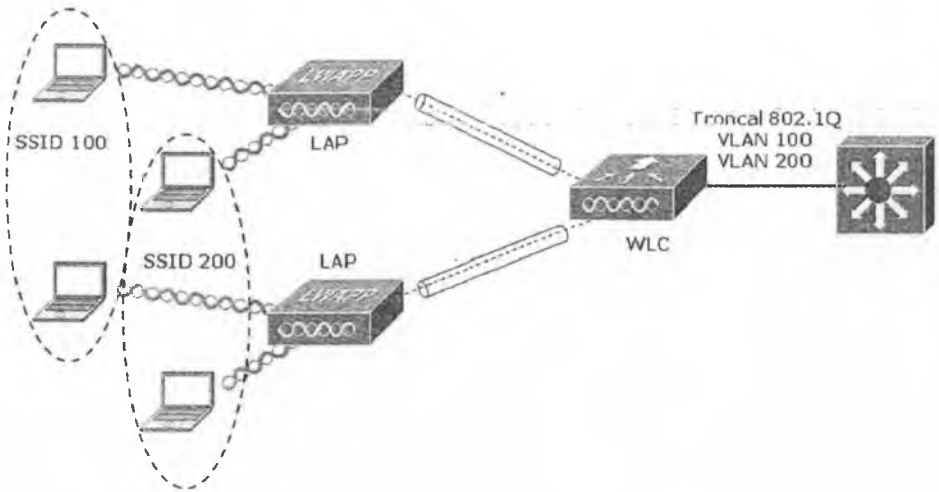
A diferencia de las otras versiones de Wi-Fi, 802.11n puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a). Gracias a ello, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada y en 802.11n permite alcanzar un mayor rendimiento. Ofrece una velocidad teórica máxima de **248 Mbps**.

6.2.5 Alianza Wi-Fi

La alianza Wi-Fi es una asociación internacional sin ánimo de lucro, formada en 1999, para certificar interoperabilidad entre productos WLAN basados en la especificación IEEE 802.11. El logotipo **Wi-Fi CERTIFIED** viene de la alianza Wi-Fi e indica que el producto ha cumplido con rigurosas pruebas de interoperabilidad, para asegurar que aquellos de diferentes proveedores operen de manera adecuada en conjunto. Otra de las actividades de esta alianza involucra el trabajo activo en la creación de nuevos y más robustos estándares de seguridad.

6.3 FUNCIONAMIENTO Y DISPOSITIVOS WLAN

Una red inalámbrica puede constar de tan solo dos dispositivos. Los nodos pueden ser simples estaciones de trabajo de escritorio o portátiles. Equipada con NIC inalámbricas, se puede establecer una red del tipo "ad-hoc" comparable a una red cableada par a par o punto a punto. Ambos dispositivos funcionan como servidores y clientes en este entorno. Aunque brinda conectividad, la seguridad es mínima, al igual que la tasa de transferencia.



En una red no siempre los dispositivos pueden ser totalmente inalámbricos

Para resolver posibles problemas de compatibilidad y mejorar operatividad, se suele instalar un punto de acceso (AP) para que actúe como hub central dentro de la infraestructura de la WLAN. El AP se conecta mediante cableado a la LAN tradicional a fin de proporcionar acceso a Internet y conectividad a la red cableada. Los AP están equipados con antenas y brindan conectividad inalámbrica a un área específica que recibe el nombre de celda. Según la composición estructural del lugar donde se instaló el AP y del tamaño y ganancia de las antenas, el tamaño de la celda puede variar enormemente. Para brindar servicio a áreas más extensas, es posible instalar múltiples puntos de acceso con cierto grado de superposición. Esta superposición permite pasar de una celda a otra (**roaming**). Esto es muy parecido a los servicios que brindan las empresas de teléfonos móviles. La superposición, en redes con múltiples puntos de acceso, es fundamental para permitir el movimiento de los dispositivos dentro de la WLAN.

Cuando se activa un cliente dentro de la WLAN, la red comenzará a escuchar para ver si hay un dispositivo compatible con el cual asociarse. Esto se conoce como escaneo y puede ser activo o pasivo.

El escaneo activo hace que se envíe un pedido de sondeo desde el nodo inalámbrico que busca conectarse a la red. Este pedido de sondeo incluirá el Identificador del Servicio (SSID) de la red a la que se desea conectar. Cuando se encuentra un AP con el mismo **SSID**, el AP emite una respuesta de sondeo. Se completan los pasos de autenticación y asociación.

Los nodos de escaneo pasivo esperan las tramas de administración (beacons) que son transmitidas por el AP (modo de infraestructura) o nodos pares (ad-hoc). Cuando un nodo recibe un beacon que contiene el SSID de la red a la que se está tratando de conectar, se realiza un intento de conexión a la red. El escaneo pasivo es un proceso continuo y los nodos pueden asociarse o desasociarse de los AP con los cambios en la potencia de la señal.

Una vez establecida la conectividad con la WLAN, un nodo transmitirá las tramas de igual forma que en cualquier otra red 802. Cuando un nodo fuente envía una trama, el nodo receptor devuelve un acuse de recibo positivo (ACK). Esto puede consumir un 50% del ancho de banda disponible. Este gasto, al combinarse con el del protocolo de prevención de colisiones, reduce la tasa de transferencia de datos a casi un 50% de su valor real. El rendimiento de la red también estará afectado por la potencia de la señal y por la degradación de la calidad de la señal debido a la distancia o interferencia.

6.4 RADIOFRECUENCIA EN WLAN

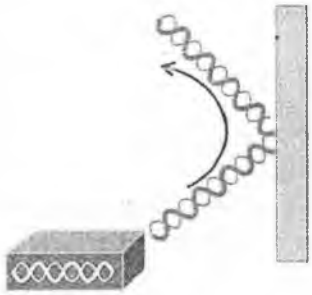
Muchas comunicaciones de WLAN ocurren dentro de la banda de 2,4 GHz comprendido en un rango de 2,412 a 2,484 GHz; mientras que otras utilizan una banda de 5 GHz en un rango de 5,150 a 5,825 GHz.

El principio de la modulación WLAN es empaquetar tantos datos como sean posibles dentro de una señal y de esa manera minimizar las posibles pérdidas por interferencias o ruidos. Cuando los datos se pierden deben ser retransmitidos utilizando más recursos.

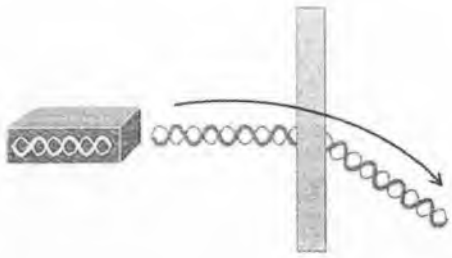
Aunque el receptor espera encontrar la portadora en una frecuencia fija, la modulación hace que la portadora varíe cada cierto tiempo. Esta variación de la frecuencia de la portadora se llama canal, a la que se hace referencia con un tipo de numeración. Los canales WLAN están definidos en el estándar 802.11.

Las características de una señal de RF pueden variar según el medio que atraviesa, por interferencias electromagnéticas, ruidos, señales de otras RF, teléfonos inalámbricos, microondas, etc. Algunas otras causas son las siguientes:

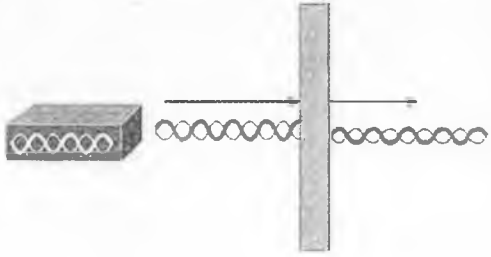
- **Reflexión**: la RF viaja a través del aire como una onda, si se encontrase con un material reflectivo la señal puede ser reflejada o rebotada.



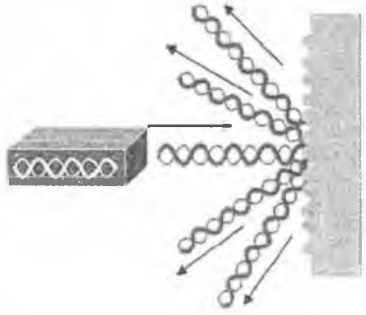
- **Refracción**: cuando la señal RF atraviesa cuerpos de diferentes densidades puede ser refractada, reduciendo la calidad y la velocidad de la onda.



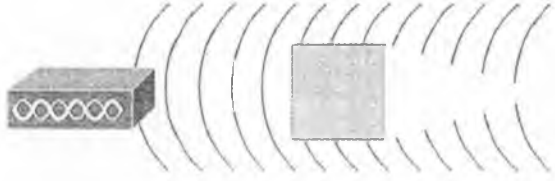
- **Absorción**: cuando una señal de RF atraviesa un material que pueda absorber su energía la señal será atenuada; cuanto más denso sea el material más atenuación sufrirá la señal.



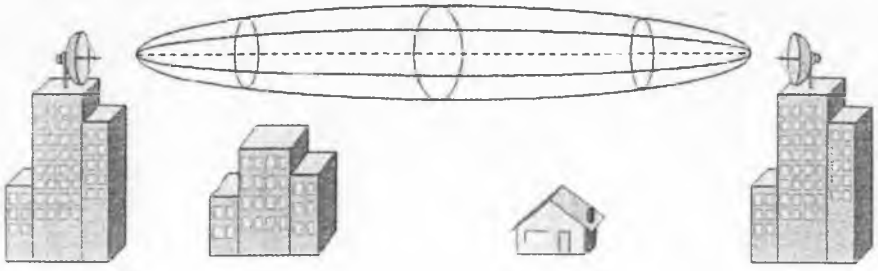
- **Dispersión**: cuando la señal RF se topa con un medio muy denso o irregular puede dispersarse en diferentes direcciones.



- **Difracción**: cuando la señal de RF se topa con un objeto que puede interrumpir o absorber intensidad podría crear una zona muerta en la cobertura.



- **Zonas de Fresnel**: uno de los factores que influyen en una señal de radio es la distancia que debe sortear hasta el destino. Técnicamente la zona Fresnel es el volumen de espacio entre emisor y receptor de RF, de manera que el desfase entre las ondas en dicho volumen no supere los 180°.



Algunos de los factores que se deben tener en cuenta en las zonas Fresnel pueden ser:

- Utilización de antenas correctas.
- Ausencia de condiciones climatológicas adversas.
- Visión directa.
- Altura correcta de las antenas.

6.4.1 Medición de la señal de radio frecuencia

Una señal de RF puede ser medida en función de su potencia o energía en unidades de **Watts (W)** o **miliwatt**, que es una milésima parte de un Watt. Por ejemplo, un teléfono móvil puede tener una potencia aproximada de 200 mW y un punto de acceso WLAN entre 1 y 100 mW.

Los valores de potencia pueden variar en un amplio rango, las comparaciones y los cálculos son complicados. Los decibelios (**dB**) se utilizan para manejar volúmenes de potencia a partir de una referencia conocida. Son logaritmos representados en un amplio rango de valores en una escala lineal.

Para el cálculo del volumen de potencia en dB se utiliza la siguiente fórmula:

$$dB = 10\log_{10}\left(\frac{P_{señal}}{P_{referencia}}\right)$$

Donde la señal de referencia puede ser comparada en 1 mW o en 1 W. Para cualquiera de los casos la abreviatura de los decibelios puede ser:

- **dBm**, referenciada con 1 Mw.
- **dBw**, referenciada con 1 W.

La potencia utilizada en las WLAN ronda los 100 mW o menos, por lo tanto se utiliza la abreviatura **dBm**.

6.5 AUTENTICACIÓN Y ASOCIACIÓN

La autenticación de las WLAN se produce en la capa 2 del modelo OSI. Es el proceso de autenticar el dispositivo no al usuario. Este es un punto fundamental a tener en cuenta con respecto a la seguridad, detección de fallos y administración general de una WLAN.

El proceso se inicia cuando el cliente envía una trama de petición de autenticación al **AP** y éste acepta o rechaza la trama. El cliente recibe una respuesta por medio de una trama de respuesta de autenticación. También puede configurarse el AP para derivar la tarea de autenticación a un servidor de autenticación, que realizaría un proceso de credencial más exhaustivo.

La asociación que se realiza después de la autenticación es el estado que permite que un cliente use los servicios del AP para transferir datos.

Tipos de autenticación y asociación:

- **No autenticado y no asociado**: el nodo está desconectado de la red y no está asociado a un punto de acceso.
- **Autenticado y no asociado**: el nodo ha sido autenticado en la red pero todavía no ha sido asociado al punto de acceso.
- **Autenticado y asociado**: el nodo está conectado a la red y puede transmitir y recibir datos a través del punto de acceso.

6.6 MÉTODOS DE AUTENTICACIÓN

6.6.1 WEP

WEP (*Wired Equivalency Privacy*) es un sistema de cifrado incluido en el estándar 802.11 como protocolo para redes Wireless que permite encriptar la información que se transmite. Proporciona encriptación a nivel 2. Está basado en el

algoritmo de encriptación RC4, y utiliza claves de 64, 128 o 256 bits. Es poco seguro debido a su arquitectura, por lo que al aumentar los tamaños de las claves de encriptación solo aumenta el tiempo necesario para romperlo.

6.6.2 WPA

WPA (*Wi-Fi Protected Access* - Acceso protegido Wi-Fi) es un sistema para asegurar redes inalámbricas, creado para corregir las carencias de seguridad de WEP; los investigadores han encontrado varias debilidades en WEP (tal como un ataque estadístico que permite recuperar la clave WEP). WPA implementa la mayoría del estándar **IEEE 802.11i**, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era preparado.

WPA fue diseñado para utilizar un servidor de autenticación (normalmente un servidor RADIUS), que distribuye claves diferentes a cada usuario; sin embargo, también se puede utilizar en un modo menos seguro de clave pre-compartida (**PSK**, *Pre-Shared Key*). La información es cifrada utilizando el algoritmo RC4, con una clave de 128 bits y un vector de inicialización de 48 bits.

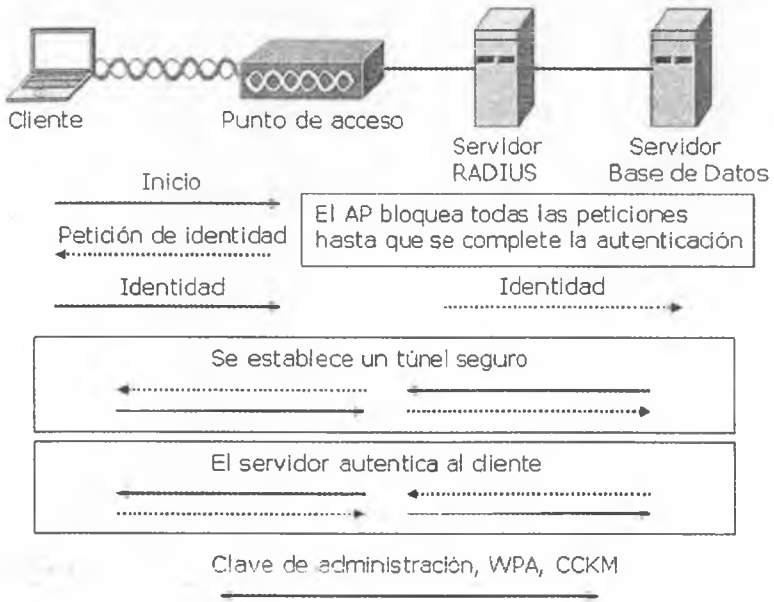
Una de las mejoras sobre WEP es dada por el Protocolo de Integridad de Clave Temporal (**TKIP**, *Temporal Key Integrity Protocol*), que cambia claves dinámicamente a medida que el sistema es utilizado. Cuando esto se combina con un vector de inicialización (IV) mucho más grande, evita los ataques de recuperación de clave (ataques estadísticos) a los que es susceptible WEP.

Adicionalmente a la autenticación y cifrado, WPA también mejora la integridad de la información cifrada. El comparador de redundancia cíclica (CRC) utilizado en WEP es inseguro, ya que es posible alterar la información y actualizar el CRC del mensaje sin conocer la clave WEP. WPA implementa un chequeo de integridad del mensaje llamado **Michael**. Además WPA incluye protección contra ataques de repetición, ya que incluye un contador de tramas.

Al incrementar el tamaño de las claves, el número de llaves en uso, y al agregar un sistema de verificación de mensajes, WPA hace que la entrada no autorizada a redes inalámbricas sea mucho más difícil. El algoritmo Michael fue el más fuerte que los diseñadores de WPA pudieron crear, bajo la premisa de que debía funcionar en las tarjetas de red inalámbricas más viejas; sin embargo es susceptible a ataques. Para limitar este riesgo, las redes WPA se desconectan durante 30 segundos cada vez que se detecta un intento de ataque.

6.6.3 WPA-2

WPA-2 está basada en el nuevo estándar IEEE 802.11i. WPA, por ser una versión previa, que se podría considerar de migración, no soporta todas las características, mientras que WPA-2 ya implementa el estándar completo. Particularmente WPA no se puede utilizar en redes ad-hoc.



Secuencia de autenticación a través de un servidor RADIUS

6.7 CASO PRÁCTICO

6.7.1 Configuración básica de un punto de acceso

La configuración básica de un AP puede resumirse en los siguientes pasos:

1. Compruebe la conexión local y si se utiliza **DHCP**. Verifique qué tipo de direccionamiento IP utilizará, tenga en cuenta la máscara y el gateway.

2. Instale el punto de acceso. Conecte el AP en la red, compruebe con un ping su correcta conectividad.

3. Configure el **SSID** en el punto de acceso, que luego utilizará el cliente.

4. Instale y configure a un cliente inalámbrico. Configure en los ordenadores correspondientes las direcciones IP y las respectivas asociaciones.

5. Verifique el funcionamiento de la red inalámbrica. Establecida la conexión la red ya es funcional.

6. Configure la seguridad **WPA-2** con **PSK**.

7. Verifique el funcionamiento de la red inalámbrica. Una vez configurados los parámetros de seguridad vuelva a verificar el correcto funcionamiento de la red.

Captura de pantalla de un AP para la configuración IP

Captura de pantalla de un AP para la configuración del SSID

Captura de pantalla de un AP para la configuración de autenticación.

6.8 FUNDAMENTOS PARA EL EXAMEN

- Estudie los conceptos básicos sobre las WLAN.
- Analice las diferencias y similitudes entre CSMA/CD y CSMA/CA.

- Estudie detalladamente los estándares 802.11.
- Recuerde qué es la alianza Wi-Fi.
- Recuerde y analice el funcionamiento de los dispositivos inalámbricos.
- Estudie y analice la implementación de las políticas de seguridad y autenticación, métodos y protocolos.

Capítulo 7

LISTAS DE ACCESO

7.1 CRITERIOS DE FILTRADO

Desde la primera vez que se conectaron varios sistemas para formar una red, ha existido una necesidad de restringir el acceso a determinados sistemas o partes de la red por motivos de seguridad, privacidad y otros. Mediante la utilización de las funciones de filtrado de paquetes del software IOS, un administrador de red puede restringir el acceso a determinados sistemas, segmentos de red, rangos de direcciones y servicios, basándose en una serie de criterios. La capacidad de restringir el acceso cobra mayor importancia cuando la red de una empresa se conecta con otras redes externas, como otras empresas asociadas o Internet.

7.1.1 Administración básica del tráfico IP

Los routers se sirven de las listas de control de acceso (ACL) para identificar el tráfico. Esta identificación puede usarse después para filtrarlo y conseguir una mejor administración del tráfico global de la red. Las listas de acceso constituyen una eficaz herramienta para el control de la red. Las listas de acceso añaden la flexibilidad necesaria para filtrar el flujo de paquetes que entra y sale de las diferentes interfaces del router.

El filtrado de paquetes permite controlar el movimiento de estos dentro de la red. Este control puede ayudar a limitar el tráfico originado por el propio router.

Una lista de acceso IP es un listado secuencial de condiciones de permiso o prohibición que se aplican a direcciones IP o a protocolos IP de capa superior.

Las listas de acceso identifican el tráfico que ha de ser filtrado en su tránsito por el router, pero no pueden filtrar el tráfico originado por el propio router.

Las listas de acceso pueden aplicarse también a los puertos de líneas de terminal virtual para permitir y denegar tráfico Telnet entrante o saliente, no es posible bloquear el acceso Telnet desde el mismo router.

Se pueden usar listas de acceso IP para establecer un control más fino o la hora de separar el tráfico en diferentes colas de prioridades y personalizadas. Una lista de acceso también puede utilizarse para identificar el tráfico "interesante" que sirve para activar las llamadas del enrutamiento por llamada telefónica bajo demanda (DDR). Las listas de acceso son mecanismos opcionales del software Cisco IOS que pueden ser configurados para filtrar o verificar paquetes con el fin de determinar si deben ser retransmitidos hacia su destino, o bien descartados.

Cuando un paquete llega a una interfaz, el router comprueba si el paquete puede ser retransmitido verificando su tabla de enrutamiento. Si no existe ninguna ruta hasta la dirección de destino, el paquete es descartado. A continuación, el router comprueba si la interfaz de destino está agrupada en alguna lista de acceso. De no ser así, el paquete puede ser enviado al búfer de salida. Si el paquete de salida está destinado a un puerto, que no ha sido agrupado a ninguna lista de acceso de salida, dicho paquete será enviado directamente al puerto destinado. Si el paquete de salida está destinado a un puerto que ha sido agrupado en una lista de acceso saliente, antes de que el paquete pueda ser enviado al puerto destinado será verificado por una serie de instrucciones de la lista de acceso asociada con dicha interfaz. Dependiendo del resultado de estas pruebas, el paquete será admitido o denegado.

Para las listas salientes, un **permit** significa enviar al búfer de salida, mientras que **deny** se traduce en descartar el paquete.

Para las listas entrantes un permit significa continuar el procesamiento del paquete tras su recepción en una interfaz, mientras que deny significa descartar el paquete.

Cuando se descarta un paquete IP, ICMP devuelve un paquete especial notificando al remitente que el destino ha sido inalcanzable.

7.1.2 Prueba de las condiciones de una ACL

Las instrucciones de una lista de acceso operan en un orden lógico secuencial. Evalúan los paquetes de principio a fin, instrucción a instrucción. Si la cabecera de un paquete se ajusta a una instrucción de la lista de acceso, el resto de las instrucciones de la lista serán omitidas, y el paquete será permitido o denegado según se especifique en la instrucción competente.

Si la cabecera de un paquete no se ajusta a una instrucción de la lista de acceso, la prueba continúa con la siguiente instrucción de la lista.

El proceso de comparación sigue hasta llegar al final de la lista, cuando el paquete será denegado implícitamente.

Una vez que se produce una coincidencia, se aplica la opción de permiso o denegación y se pone fin a las pruebas de dicho paquete. Esto significa que una condición que deniega un paquete en una instrucción no puede ser afinada en otra instrucción posterior.

La implicación de este modo de comportamiento es que el orden en que figuran las instrucciones en la lista de acceso es esencial. Hay una instrucción final que se aplica a todos los paquetes que no han pasado ninguna de las pruebas anteriores. Esta condición final se aplica a todos esos paquetes y se traduce en una condición de denegación del paquete.

En lugar de salir por alguna interfaz, todos los paquetes que no satisfacen las instrucciones de la lista de acceso son descartados.

Esta instrucción final se conoce como la denegación implícita de todo, al final de cada lista de acceso. Aunque esta instrucción no aparece en la configuración del router, siempre está activa. Debido a dicha condición, es necesario que en toda lista de acceso exista al menos una instrucción permit, en caso contrario la lista de acceso bloquearía todo el tráfico.

7.2 TIPOS DE LISTAS DE ACCESO

7.2.1 Listas de acceso estándar

Las listas de acceso estándar solo comprueban las direcciones de origen de los paquetes que solicitan enrutamiento. El resultado es el permiso o la denegación de la salida del paquete por parte del protocolo, basándose en la dirección IP de la red-subred-host de origen.

7.2.2 Listas de acceso extendidas

Las listas de acceso extendidas comprueban tanto la dirección de origen como la de destino de cada paquete. También pueden verificar protocolos especificados, números de puerto y otros parámetros.

7.2.3 Listas de acceso con nombre

Permiten asignar nombres en lugar de un rango numérico en las listas de acceso estándar y extendidas.

7.3 APLICACIÓN DE UNA LISTA DE ACCESO

Las listas de acceso expresan el conjunto de reglas que proporcionan un control añadido para los paquetes que entran en interfaces de entrada, paquetes que se trasmiten por el router y paquetes que salen de las interfaces de salida del router.

Una vez creada, una ACL debe asociarse a una o varias interfaces de forma que analice todos los paquetes que pasen por estas ya sea de manera entrante o saliente según corresponda el caso. La manera de determinar cuál de los casos es el que corresponde es pensar si los paquetes van hacia la red en cuestión (saliente) o si vienen de ella (entrante).

Las ACL deben ubicarse donde más repercutan sobre la eficacia. Las reglas básicas son:

- Ubicar las ACL extendidas lo más cerca posible del origen del tráfico denegado. De esta manera, el tráfico no deseado se filtra sin atravesar la infraestructura de red.

- Como las ACL estándar no especifican las direcciones de destino, colóquelas lo más cerca del destino posible.

7.3.1 Lista de acceso entrante

Los paquetes entrantes son procesados antes de ser enrutados a una interfaz de salida, si el paquete pasa las pruebas de filtrado, será procesado para su enrutamiento (evita la sobrecarga asociada a las búsquedas en las tablas de enrutamiento si el paquete ha de ser descartado por las pruebas de filtrado).

Procesamiento de una ACL entrante, el paquete entrante es filtrado antes de su enrutamiento

7.3.2 Lista de acceso saliente

Los paquetes entrantes son enrutados a la interfaz de salida y después son procesados por medio de la lista de acceso de salida antes de su transmisión.

Procesamiento de una ACL saliente, el paquete saliente debe ser enrutado antes de su respectivo filtrado

NOTA:

El estudio de este libro se basa en las listas de acceso IP.

RECUERDE:

Las listas de acceso no actúan sobre paquetes originados en el propio router, como las actualizaciones de enrutamiento a las sesiones telnet salientes.

7.4 MÁSCARA COMODÍN

Puede ser necesario probar condiciones para un grupo o rango de direcciones IP, o bien para una dirección IP individual. La comparación de direcciones tiene lugar usando máscaras que actúan a modo de comodines en las direcciones de la lista de acceso, para identificar los bits de la dirección IP que han de coincidir explícitamente y cuáles pueden ser ignorados. El enmascaramiento wildcard para los bits de direcciones IP utiliza los números 1 y 0 para referirse a los bits de la dirección. Teniendo en cuenta que:

- Un bit de máscara wildcard **0** significa "comprobar el valor correspondiente".
- Un bit de máscara wildcard **1** significa "No comprobar (ignorar) el valor del bit correspondiente".

Para los casos más frecuentes de enmascaramiento wildcard se pueden utilizar abreviaturas.

- **Host** = máscara comodín 0.0.0.0, utilizada para un host específico.
- **Any** = 0.0.0.0 255.255.255.255, utilizado para definir a cualquier host, red o subred.

En el caso de permitir o denegar redes o subredes enteras se deben ignorar todos los host pertenecientes a dicha dirección de red o subred. Cualquier dirección de host será leída como dirección de red o subred. Por ejemplo, el siguiente caso:

Dirección IP	172	16	32	0
En binarios	**10101100**	**00010000**	**00100000**	**00000000**
Máscara de red	**11111111**	**11111111**	**11100000**	**00000000**
wildcard	**00000000**	**00000000**	**00011111**	**11111111**
Resultado	Se tienen en cuenta 8 bits	Se tienen en cuenta 8 bits	Se tienen en cuenta 3 bits, se ignoran 5	Ignorados

Wildcard: 0.0.31.255

Cálculo rápido:

Reste la máscara de subred 255.255.224.0 al valor 255.255.255.255:

```
 255.255.255.255
-255.255.224.000
 000.000.031.255
```

El resultado es la máscara wildcard **0.0.31.255**.

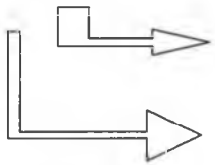
7.5 CASO PRÁCTICO

7.5.1 Cálculo de wilcard

Las wildcard también permiten identificar rangos simplificando la cantidad de comandos a introducir, en este ejemplo la wildcard debe identificar el rango de subredes entre la 172.16.16.0/24 y la 172.16.31.0/24.

Trabaje con el tercer octeto, se debe trabajar con el rango entra 16 y 31:

16	000	1	0000
17	000	1	0001
18	000	1	0010
19	000	1	0011
20	000	1	0100
21	000	1	0101
22	000	1	0110
...	...	.	....
30	000	1	1110
31	000	1	1111



Los bits a ignorar junto con los del cuarto octeto estarán en 1
[00001111.11111111 = 15.255]

El bit común es el correspondiente al valor decimal 16,

por lo tanto, la Wildcard será:

172.16.16.0 0.0.15.255

7.6 PROCESO DE CONFIGURACIÓN DE ACL

El proceso de creación de una ACL se lleva a cabo creando la lista y posteriormente asociándola a una interfaz entrante o saliente.

7.6.1 Listas de acceso numeradas

Las ACL numeradas llevan un número identificativo que las identifica según sus características. La siguiente tabla muestra los rangos de listas de acceso numeradas:

ACL	Rango	Rango extendido
IP estándar	1-99	1300-1999
IP extendida	100-199	2000-2699
Prot, type code	200-299	
DECnet	300-399	
XNS estándar	400-499	
XNS extendida	500-599	
Apple Talk	600-699	
. . . . .	. . . . .	
IPX estándar	800-899	
IPX extendida	900-999	
Filtros Sap	1000-1099	
. . . . .	. . . . .	

7.6.2 Configuración de ACL estándar

Las listas de acceso IP estándar verifican solo la dirección de origen en la cabecera del paquete IP(capa 3).

```
Router(config)#access-list[1-99][permit|deny][dirección de
origen][máscara comodín]
```

Donde:

- **1-99**: identifica el rango y número de lista.
- **Permit|deny**: indica si esta entrada permitirá o bloqueará el tráfico a partir de la dirección origen.
- **Dirección de origen**: identifica la dirección IP de origen.

- **Máscara comodín** (wildcard): identifica los bits del campo de la dirección que serán comprobados.

NOTA:

La máscara predeterminada es 0.0.0.0 (coincidencia de todos los bits).

7.6.3 Asociación de la ACL estándar a una interfaz

Una vez configurada asocie la ACL estándar a la interfaz a través del siguiente comando dentro del modo de dicha interfaz.

```
Router(config-if)#ip access-group[N° de lista de acceso][in|out]
```

Donde:

- **Número de lista de acceso**: indica el número de lista de acceso que será aplicada a esa interfaz.
- **In|out**: selecciona si la lista de acceso se aplicará como filtro de entrada o de salida.

7.6.4 Configuración de ACL extendida

Las listas de acceso IP extendidas pueden verificar otros muchos elementos, incluidas opciones de la cabecera del segmento (capa 4), como los números de puerto.

- Direcciones IP de origen y destino, protocolos específicos.
- Números de puerto TCP y UDP.

El proceso de configuración de una ACL IP extendida es el siguiente:

```
Router(config)#access-list[100-199][permit|deny][protocolo]
[dirección de origen][máscara comodín][dirección de destino]
[máscara comodín][puerto][establisehed][log]
```

- **100-199**: identifica el rango y número de lista.

- **Permit|deny**: indica si la entrada permitirá o bloqueará el tráfico desde la dirección origen hacia el destino.

- **Protocolo**: como por ejemplo IP, TCP, UDP, ICMP.

- **Dirección origen, dirección destino**: identifican direcciones IP de origen y destino.

- **Máscara comodín**: son las máscaras wildcard. Identifica los bits del campo de la dirección que serán comprobados.

- **Puerto** (opcional): puede ser, por ejemplo, lt (menor que), gt (mayor que), eq (igual a), o neq (distinto que) y un número de puerto de protocolo correspondiente.

- **Establisehed** (opcional): se usa solo para TCP de entrada. Esto permite que el tráfico TCP pase si el paquete utiliza una conexión ya establecida (por ejemplo, posee un conjunto de bits ACK).

- **Log** (opcional): envía un mensaje de registro a la consola a un servidor syslog determinado.

Algunos de los números de puerto más conocidos, se detallan con mayor profundidad más adelante:

21	FTP
23	TELNET
25	SMTP
69	TFTP
53	DNS
80	HTTP
109	POP 2

7.6.5 Asociación de las ACL extendida a una interfaz

La asociación de las ACL a una interfaz en particular se realiza en el modo de interfaz aplicando el siguiente comando.

```
Router(config-if)#ip access-group[N° de lista de acceso][in|out]
```

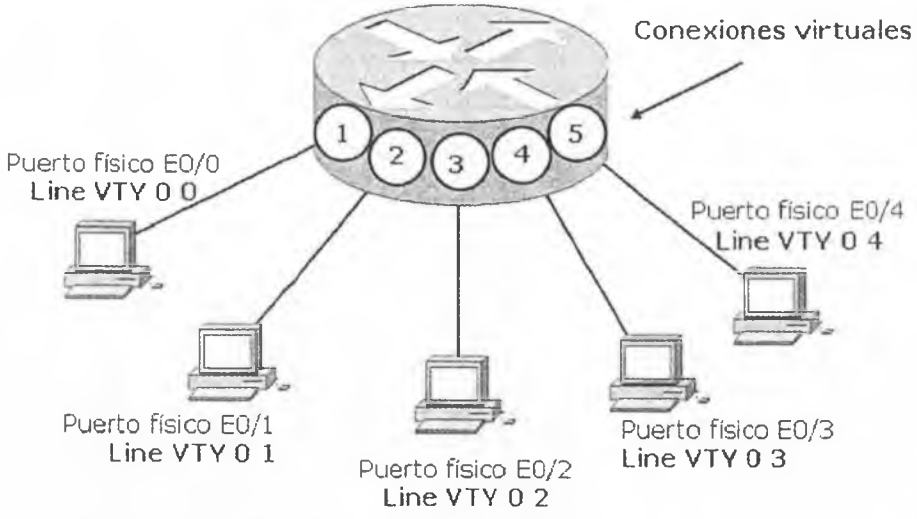
Donde:

- **Número de lista de acceso**: indica el número de lista de acceso que será aplicada a esa interfaz.
- **In|out**: selecciona si la lista de acceso se aplicará como filtro de entrada o de salida.

7.6.6 Aplicación de una ACL a la línea de telnet

Para evitar intrusiones no deseadas en las conexiones de telnet se puede crear una lista de acceso estándar y asociarla a la Line VTY. El proceso de creación se lleva a cabo como una ACL estándar denegando o permitiendo un origen hacia esa interfaz. El modo de asociar la ACL a la Línea de telnet es el siguiente:

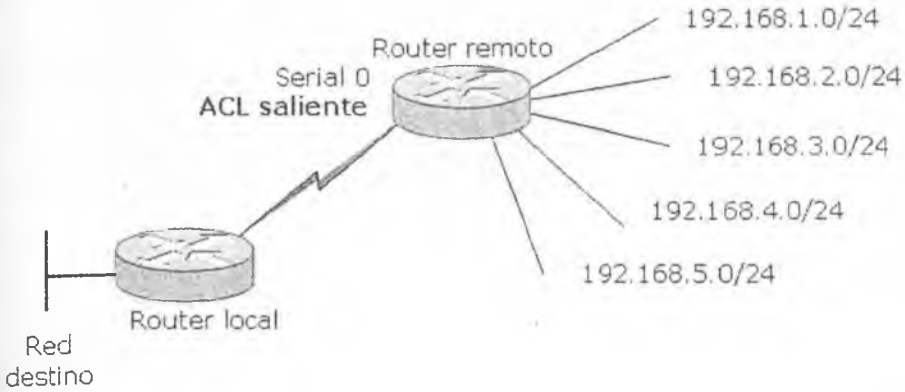
```
router(config)#line vty 0 4
router(config-line)#access-class[N° de lista de acceso][in|out]
```



7.7 CASO PRÁCTICO

7.7.1 Configuración de una ACL estándar

Se ha denegado en el router remoto la red 192.168.1.0 y luego se ha permitido a cualquier origen, posteriormente se asoció la ACL a la interfaz Serial 0/0 como saliente.

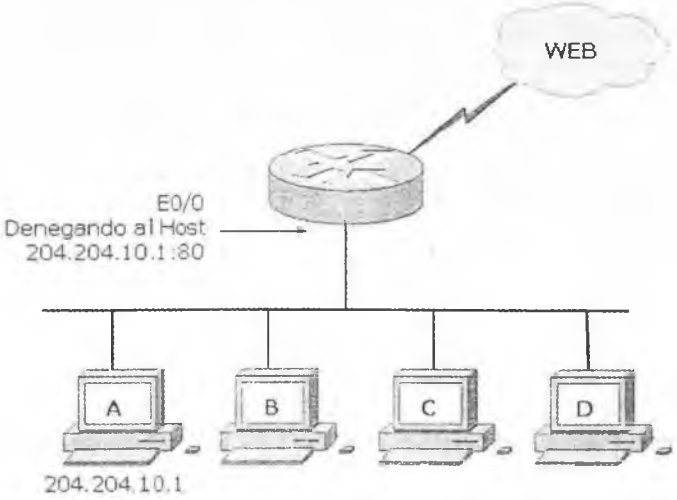



```
Router#configure terminal
Router(config)#access-list 10 deny 192.168.1.0 0.0.0.0
Router(config)#access-list 10 permit any
Router(config)#interface serial 0/0
Router(config-if)#ip access-group 10 out
```

7.7.2 Configuración de una ACL extendida

Se ha denegado al host A, 204.204.10.1 (identificándolo con la abreviatura "host") hacia el puerto 80 de cualquier red de destino (usando el término any). Posteriormente se permite todo tráfico IP. Esta ACL se asoció a la interfaz ethernet 0/1 como entrante.

```
Router(config)#access-list 120 deny tcp host 204.204.10.1  any eq 80
Router(config)#access-list 120 permit ip any any
Router(config)#interface ethernet 0/1
Router(config-if)#ip access-group 120 in
```



7.7.3 Configuración de ACL con subred

En el siguiente caso la subred 200.20.10.64/29 tiene denegado el acceso de todos sus hosts en el protocolo UDP, mientras que los restantes protocolos y otras subredes tienen libre acceso. La ACL es asociada a la ethernet 0/0 como entrante. Observe la wilcard utilizada en este caso.

```
Router(config)#access-list 100 deny udp 200.20.10.64 0.0.0.7 any
Router(config)#access-list 100 permit ip any any
Router(config)#interface ethernet 0/0
Router(config-if)#ip access-group 100 in
```

Procedimiento para hallar la máscara comodín de la subred:

200.200.10.64/29 es lo mismo que 200.200.10.64 255.255.255.248

255.255.255.255
255.255.255.248
000.000.000.007

Wilcard: 0.0.0.7

RECUERDE:

Al final de cada ACL existe una negación implícita. Debe existir al menos un permit.

7.8 BORRADO DE LAS LISTAS DE ACCESO

Desde el modo interfaz donde se aplicó la lista desasociar dicha ACL. Tenga en cuenta que en una interfaz puede tener asociadas varias ACL.

```
Router(config-if)#no ip access-group[N° de lista de acceso]
```

Posteriormente desde el modo global elimine la ACL:

```
router(config)#no access-list[N° de lista de acceso]
```

7.9 LISTAS DE ACCESO IP CON NOMBRE

Con listas de acceso IP numeradas, para modificar una lista tendría que borrar primero la lista de acceso y volver a introducirla de nuevo con las correcciones necesarias.

En una lista de acceso numerada no es posible borrar instrucciones individuales. Las listas de acceso IP con nombre permiten eliminar entradas individuales de una lista específica. El borrado de entradas individuales permite modificar las listas de acceso sin tener que eliminarlas y volver a configurarlas desde el principio. Sin embargo, no es posible insertar elementos selectivamente en una lista.

7.9.1 Configuración de una lista de acceso nombrada

Básicamente, la configuración de una ACL nombrada es igual a las extendidas o estándar numeradas. Si se agrega un elemento a la lista, este se coloca al final de la misma. No es posible usar el mismo nombre para varias listas de acceso. Las listas de acceso de diferentes tipos tampoco pueden compartir nombre.

```
Router(config)#ip access-list[standard|extended] nombre
Router(config[std|ext]nacl)#[permit|deny] [condiciones de prueba]
Router(config)#Interfaz asociación de la ACL
Router(config-if)#ip access-group nombre [in|out]
```

Para eliminar una instrucción individual, anteponga no a la condición de prueba.

```
Router(config[std|ext]nacl)#no[permit|deny][condiciones de prueba]
```

7.10 CASO PRÁCTICO

7.10.1 Configuración de una ACL nombrada

Se creó una ACL con el nombre INTRANET que deniega todo tráfico de cualquier origen a cualquier destino hacia el puerto 21, luego se permite cualquier otro tráfico IP. Se usó el comando log (opcional) para enviar información de la ACL a un servidor. Se asocia a la interfaz ethernet 1 como saliente.

```
Router(config)#ip access-list extended INTRANET
Router(config-ext-nacl)#deny tcp any any eq 21 log
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#exit
Router(config)#interface ethernet 1
Router(config-if)#ip access-group INTRANET out
```

7.11 COMENTARIOS EN LAS ACL

Las ACL permiten agregar comentarios para facilitar su comprensión o funcionamiento. El comando remark no actúa sobre las sentencias de las ACL pero brindan a los técnicos la posibilidad de una visión rápida sobre la actividad de las listas.

Los comentarios pueden agregarse tanto a las ACL nombradas como también a las numeradas, la clave reside en agregar los comentarios antes de la configuración de los permisos o denegaciones.

La sintaxis muestra una ACL nombrada con el comando remark:

```
Router(config)#ip access-list[standard|extended] nombre
Router(config[std|ext]nacl)#remark comentario
```

La sintaxis muestra una ACL numerada con el comando remark:

```
Router(config)#ip access-list [número] remark comentario
```

7.12 OTROS TIPOS DE LISTAS DE ACCESO

7.12.1 Listas de acceso dinámicas

Este tipo de ACL depende de telnet a partir de la autenticación de los usuarios que quieran atravesar el router y que han sido previamente bloqueados por una ACL extendida. Una ACL dinámica añadida a la ACL extendida existente permitirá tráfico a los usuarios que son autenticados en una sesión de telnet por un período de tiempo en particular.

7.12.2 Listas de acceso reflexivas

Permiten el filtrado de paquetes IP en función de la información de la sesión de capa superior. Mayormente se utilizan para permitir el tráfico saliente y para limitar el entrante en respuesta a las sesiones originadas dentro del router.

7.12.3 Listas de acceso basadas en tiempo

Este tipo de ACL permite la configuración para poner en actividad el filtrado de paquetes solo en períodos de tiempo determinados por el administrador. En algunos casos puede ser muy útil la utilización de ACL en algunos momentos del día o particularmente en solo algunos días de la semana.

7.13 PUERTOS TCP MÁS UTILIZADOS EN LAS ACL

Número de puerto	Comando	Protocolo
7	**echo**	Echo
9	**discard**	Discard
13	**daytime**	Daytime
19	**chargen**	Character Generator

20	**ftp-data**	FTP Data Connections
21	**ftp**	File Transfer Protocol
23	**telnet**	Telnet
25	**smtp**	Simple Mail Transport Protocol
37	**time**	Time
53	**domain**	Domain Name Service
43	**whois**	Nickname
49	**tacacs**	TAC Access Control System
70	**gopher**	Gopher
79	**finger**	Finger
80	**www-http**	World Wide Web
101	**hostname**	NIC Hostname Server
109	**pop2**	Post Office Protocol v2
110	**pop3**	Post Office Protocol v3
111	**sunrpc**	Sun Remote Procedure Call
113	**ident**	Ident Protocol
119	**nntp**	Network News Transport Protocol
179	**bgp**	Border Gateway Protocol
194	**irc**	Internet Relay Chat
496	**pim-auto-rp**	PIM Auto-RP
512	**exec**	Exec

513	**login**	Login
514	**cmd**	Remote commands
515	**lpd**	Printer service
517	**talk**	Talk
540	**uucp**	Unix-to-Unix Copy Program

7.14 PUERTOS UDP MÁS UTILIZADOS EN LAS ACL

Número de puerto	Comando	Protocolo
7	**echo**	Echo
9	**discard**	Discard
37	**time**	Time
42	**nameserver**	IEN116 name service
49	**tacacs**	TAC Access Control System
53	**domain**	Domain Name Service
67	**bootps**	Bootstrap Protocol server
68	**bootpc**	Bootstrap Protocol client
69	**tftp**	Trivial File Transfer Protocol
111	**sunrpc**	Sun Remote Procedure Call
123	**ntp**	Network Time Protocol
137	**netbios-ns**	NetBios name service
138	**netbios-dgm**	NetBios datagram service

139	**netbios-ss**	NetBios Session Service
161	**snmp**	Simple Network Management Protocol
162	**snmptrap**	SNMP Traps
177	**xdmcp**	X Display Manager Control Protocol
195	**dnsix**	DNSIX Security Protocol Auditing
434	**mobile-ip**	Mobile IP Registration
496	**pim-auto-rp**	PIM Auto-RP
500	**isakmp**	Internet Security Association and Key Management Protocol
512	**biff**	Biff
513	**who**	Who Service
514	**syslog**	System Logger
517	**talk**	Talk
520	**rip**	Routing Information Protocol

7.15 PROTOCOLOS MÁS UTILIZADOS EN LAS ACL

Comando	Descripción
eigrp	Cisco EIGRP routing protocol
gre	Cisco GRE tunneling
icmp	Internet Control Message Protocol
igmp	Internet Gateway Message Protocol

ip	Any Internet Protocol
ospf	OSPF routing protocol
pcp	Payload Compression Protocol
tcp	Transmission Control Protocol
udp	User Datagram Protocol

7.16 VERIFICACIÓN ACL

Verifica si una lista de acceso está asociada a una interfaz:

```
Router#show ip interface[tipo de interfaz][N° de interfaz]
```

Muestra información de la interfaz IP:

```
Router#show access-list
```

Muesta información general de las ACL y de las interfaces asociadas:

```
Router#running-config
```

Muestra contenido de todas las listas de acceso:

```
Router#show access-lists
Standard IP access list 10
    deny   192.168.1.0
Extended IP access list 120
    deny   tcp host 204.204.10.1 any eq 80
    permit ip any any
Extended IP access list INTRANET
    deny   tcp any any eq 21 log
    permit ip any any
```

```
Router#show[protocolo]access-list[N° lista de acceso|nombre]
```

RECUERDE:

Una lista de acceso puede ser aplicada a múltiples interfaces.

Solo puede haber una lista de acceso por protocolo, por dirección y por interfaz.

Es posible tener varias listas para una interfaz, pero cada una debe pertenecer a un protocolo diferente.

Organice las listas de acceso de modo que las referencias más específicas a una red o subred aparezcan delante de las más generales.

Coloque las condiciones de cumplimiento más frecuentes antes de las menos habituales.

Las adiciones a las listas se agregan siempre al final de estas, pero siempre delante de la condición de denegación implícita.

No es posible agregar ni eliminar selectivamente instrucciones de una lista cuando se usan listas de acceso numeradas, pero sí cuando se usan listas de acceso IP con nombre.

A menos que termine una lista de acceso con una condición de permiso implícito de todo, se denegará todo el tráfico que no cumpla ninguna de las condiciones establecidas en la lista al existir un deny implícito al final de cada lista.

Toda lista de acceso debe incluir al menos una instrucción permit. En caso contrario, todo el tráfico será denegado.

Cree una lista de acceso antes de aplicarla a la interfaz. Una interfaz con una lista de acceso inexistente o indefinida aplicada al mismo permitirá todo el tráfico.

Las listas de acceso permiten filtrar solo el tráfico que pasa por el router. No pueden hacer de filtro para el tráfico originado por el propio router.

RECUERDE:

El orden en el que aparecen las instrucciones en la lista de acceso es fundamental para un filtrado correcto. La práctica recomendada consiste en crear las listas de acceso usando un editor de texto y descargarlas después en un router vía TFTP o copiando y pegando el texto. Las listas de acceso se procesan de arriba a abajo. Si coloca las pruebas más específicas y las que se verificarán con más frecuencia al comienzo de la lista de acceso, se reducirá la carga de procesamiento. Solo las listas de acceso con nombre permiten la supresión, aunque no la alteración del orden de instrucciones individuales en la lista. Si desea reordenar las instrucciones de una lista de acceso, deberá eliminar la lista completa y volver a crearla en el orden apropiado o con las instrucciones correctas.

RECUERDE:

Las listas de acceso extendidas deben colocarse normalmente lo más cerca posible del origen del tráfico que será denegado, mientras que las estándar, lo más cerca posible del destino.

7.17 FUNDAMENTOS PARA EL EXAMEN

- Recuerde los fundamentos para el filtrado y administración del tráfico IP.
- Memorice las pruebas de condiciones que efectúa el router y cuáles son los resultados en cada caso.
- Estudie los tipos de ACL, su asociación con las interfaces del router y cuál es la manera más adecuada para aplicarlas.
- Estudie y analice la función de las máscaras comodín y su efecto en las ACL.
- Memorice los rangos de las ACL numeradas.
- Memorice los números de puertos básicos empleados en la configuración de las ACL.

- Recuerde que existen otros tipos de ACL, sepa cuáles son.
- Memorice los comandos para las configuraciones de todas las ACL, teniendo en cuenta las condiciones fundamentales para su correcto funcionamiento, incluidos los comandos para su visualización.
- Recuerde que existe un tipo especial de ACL para telnet.
- Ejercite todo lo que pueda con las wildcard.
- Ejercite todas las configuraciones en dispositivos reales o en simuladores.

Capítulo 8

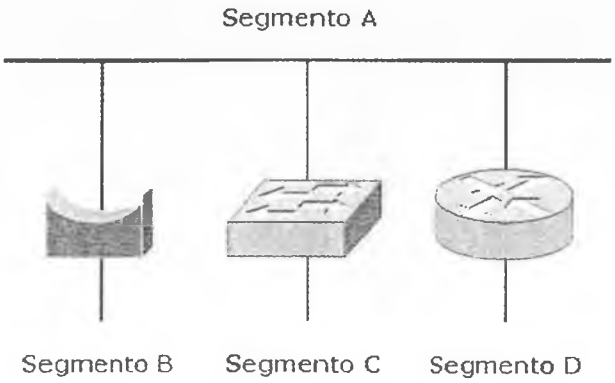
CONMUTACIÓN DE LAN

8.1 CONMUTACIÓN DE CAPA 2

Las redes ethernet pueden mejorar su desempeño a partir de la conmutación de tramas. La conmutación permite segmentar una LAN creando dominios de colisión con anchos de banda exclusivos para cada segmento pudiendo transmitir y recibir al mismo tiempo sin el retardo que provocarían las colisiones. El ancho de banda dedicado por puerto es llamado **microsegmentación**.

Los puentes, switches y routers dividen las redes en segmentos.

- Los puentes trabajan a nivel de software generando alta latencia.
- Los routers utilizan gran cantidad de recursos.
- Los switches lo hacen a nivel de hardware siendo tan rápidos como el medio lo exija.



Los puentes, switches y routers dividen las redes en segmentos

La conmutación permite:

- **Comunicaciones dedicadas entre dispositivos**. Los hosts poseen un dominio de colisión puro libre de colisiones, incrementando la rapidez de transmisión.

- **Múltiples conversaciones simultáneas**. Los hosts pueden establecer conversaciones simultáneas entre segmentos gracias a los circuitos virtuales proporcionados por los switch.

- **Comunicaciones full-duplex**. El ancho de banda dedicado por puerto permite transmitir y recibir a la vez, duplicando el ancho de banda teórico.

- **Adaptación a la velocidad del medio**. La conmutación creada por un switch funciona a nivel de hardware (ASIC), respondiendo tan rápidamente como el medio lo permita.

8.1.1 Conmutación con switch

Un switch segmenta una red en dominios de colisión, tantos como puertos activos posea. Aprender direcciones, reenviar, filtrar paquetes y evitar bucles también son funciones de un switch.

El switch segmenta el tráfico de manera que los paquetes destinados a un dominio de colisión determinado no se propaguen a otro segmento aprendiendo las

direcciones MAC de los hosts. A diferencia de un hub, un switch no inunda todos los puertos con las tramas, por el contrario el switch es selectivo con cada trama.

Debido a que los switches controlan el tráfico para múltiples segmentos al mismo tiempo, han de implementar memoria búfer para que puedan recibir y transmitir tramas independientemente en cada puerto o segmento.

Un switch nunca aprende direcciones de difusión o multidifusión, dado que las direcciones no aparecen en estos casos como dirección de origen de la trama. Una trama de broadcast será transmitida a todos los puertos a la vez.

8.2 TECNOLOGÍAS DE CONMUTACIÓN

8.2.1 Almacenamiento y envío

El switch debe recibir la trama completa antes de enviarla por el puerto correspondiente. Lee la dirección MAC destino, comprueba el **CRC** (contador de redundancia cíclica, utilizado en las tramas para verificar errores de envío), aplica los filtrados correspondientes y retransmite. Si el CRC es incorrecto, se descarta la trama. El retraso de envío o latencia suele ser mayor debido a que el switch debe almacenar la trama completa, verificarla y posteriormente enviarla al segmento correspondiente.

8.2.2 Método de corte

El switch verifica la dirección MAC de destino en cuanto recibe la cabecera de la trama, y comienza de inmediato a enviar la trama. La desventaja de este modo es que el switch podría retransmitir una trama de colisión o una trama con un valor de CRC incorrecto, pero la latencia es muy baja.

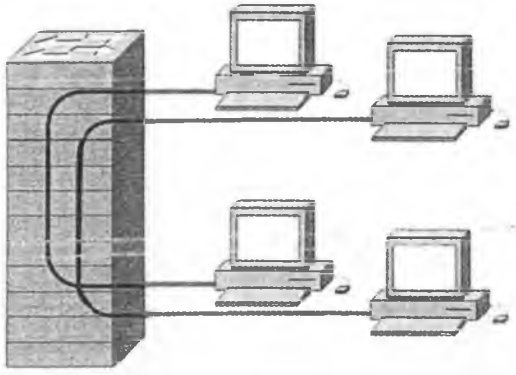
8.2.3 Libre de fragmentos

Modo de corte modificado, el switch lee los primeros 64 bytes antes de retransmitir la trama. Normalmente las colisiones tienen lugar en los primeros 64 bytes de una trama. El switch solo envía las tramas que están libres de colisiones.

8.3 APRENDIZAJE DE DIRECCIONES

Un switch crea circuitos virtuales entre segmentos, para ello debe identificar las direcciones MAC de destino, buscar en su tabla de direcciones MAC a qué puerto debe enviarla y ejecutar el envío. Cuando un switch se inicia no posee datos sobre los hosts conectados a sus puertos, por lo tanto inunda todos los puertos esperando capturar la MAC correspondiente.

A medida que las tramas atraviesan el switch, este las comienza a almacenar en la memoria **CAM** (memoria de contenido direccionable) asociándolas a un puerto de salida e indicando en cada entrada una marca horaria a fin de que pasado cierto tiempo sea eliminada preservando el espacio en memoria. Si un switch detecta que la trama pertenece al mismo segmento de donde proviene no la recibe evitando tráfico, si por el contrario el destino pertenece a otro segmento, solo enviará la trama al puerto correspondiente de salida. Si la trama fuera un broadcast, el switch inundará todos los puertos con dicha trama.



Un switch crea circuitos virtuales mapeando la dirección MAC de destino con el puerto de salida correspondiente

La siguiente captura muestra la tabla MAC de un switch:

```
switch#sh mac-address-table
Dynamic Address Count:                  172
Secure Address Count:                   0
Static Address (User-defined) Count:    0
System Self Address Count:              76
Total MAC addresses:                    248
Maximum MAC addresses:                  8192
```

```
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
0000.0c07.ac01       Dynamic         12  GigabitEthernet0/1
0000.0c07.ac0b       Dynamic         11  GigabitEthernet0/1
0000.c0e5.b8d4       Dynamic         12  GigabitEthernet0/2
0001.9757.d29c       Dynamic          1  GigabitEthernet0/1
0001.9757.d29c       Dynamic          2  GigabitEthernet0/1
0001.9757.d29c       Dynamic          3  GigabitEthernet0/1
0001.9757.d29c       Dynamic          4  GigabitEthernet0/1
0001.9757.d29c       Dynamic          5  GigabitEthernet0/1
0001.9757.d29c       Dynamic          6  GigabitEthernet0/1
0001.9757.d29c       Dynamic          7  GigabitEthernet0/1
0001.9757.d29c       Dynamic          8  GigabitEthernet0/1
0001.9757.d29c       Dynamic          9  GigabitEthernet0/1
```

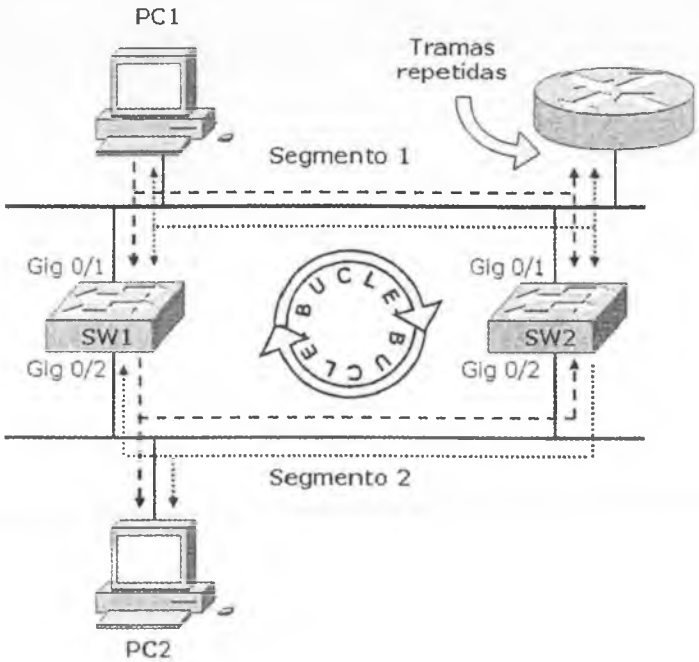
8.3.1 Bucles de capa 2

Las redes están diseñadas por lo general con enlaces y dispositivos redundantes. Estos diseños eliminan la posibilidad de que un punto de fallo individual origine al mismo tiempo varios problemas que deben ser tenidos en cuenta. Sin algún servicio que evite bucles, cada switch inundaría las difusiones en un bucle infinito. Esta situación se conoce como **bucle de puente**.

La propagación continua de estas difusiones a través del bucle produce una tormenta de difusión, lo que da como resultado un desperdicio del ancho de banda, así como impactos serios en el rendimiento de la red. Podrían ser distribuidas múltiples copias de tramas sin difusión a los puestos de destino.

Muchos protocolos esperan recibir una sola copia de cada transmisión. La presencia de múltiples copias de la misma trama podría ser causa de errores irrecuperables.

•Una inestabilidad en el contenido de la tabla de direcciones MAC da como resultado que se reciban varias copias de una misma trama en diferentes puertos del switch.



Los bucles y las tramas duplicadas son algunos de los problemas que soluciona STP.

8.4 PROTOCOLO DE ÁRBOL DE EXPANSIÓN

STP, Protocolo de Árbol de Expansión, es un protocolo de capa dos publicado en la especificación del estándar IEEE 802.1d.

El objetivo del árbol de expansión es mantener una red libre de bucles. Un camino libre de bucles se consigue cuando un dispositivo es capaz de reconocer un bucle en la topología y bloquear uno o más puertos redundantes.

El protocolo Árbol de expansión explora constantemente la red, de forma que cualquier fallo o adición en un enlace, switch o bridge es detectado al instante. Cuando cambia la topología de red, el algoritmo de árbol de expansión reconfigura los puertos del switch o el bridge para evitar una pérdida total de la conectividad.

Los switches intercambian información multicast (**BPDU**) cada dos segundos, si se detecta alguna anormalidad en algún puerto STP, cambiará de estado algún puerto automáticamente utilizando algún camino redundante sin que se pierda conectividad en la red.

Los switches solo pueden ejecutar varias instancias STP mientras que los puentes solo una. Cisco desarrolló **PVST+** para que una red pueda ejecutar una instancia de STP para cada VLAN de la red.

8.4.1 Proceso STP

STP funciona automáticamente siguiendo los siguientes criterios:

- **Elección de un switch raíz**. En un dominio de difusión solo debería existir un **switch raíz**. Todos los puertos del bridge raíz se encuentran en estado **enviando** y se denominan puertos designados. Cuando está en este estado, un puerto puede enviar y recibir tráfico. La elección de un switch raíz se lleva a cabo determinando el switch que posea la menor **prioridad**. Este valor es la suma de la prioridad por defecto dentro de un rango de 1 al 65536 (20 a 216) y el ID del switch equivalente a la dirección MAC. Por defecto la prioridad es $\mathbf{2^{15} = 32768}$ y es un valor configurable. Un administrador puede cambiar la elección del switch raíz por diversos motivos configurando un valor de prioridad menor a 32768. Los demás switches del dominio se llaman **switch no raíz**.

- **Puerto raíz**. El puerto raíz corresponde a la ruta de menor coste desde el **switch no raíz**, hasta el **switch raíz**. Los puertos raíz se encuentran en estado de envío o retransmisión y proporcionan conectividad hacia atrás al switch raíz. La ruta de menor coste al switch raíz se basa en el ancho de banda.

- **Puertos designados**. El puerto designado es el que conecta los segmentos al switch raíz y solo puede haber un puerto designado por segmento. Los puertos designados se encuentran en estado de retransmisión y son los responsables del reenvío de tráfico entre segmentos. Los puertos no designados se encuentran normalmente en estado de bloqueo con el fin de romper la topología de bucle.

NOTA:

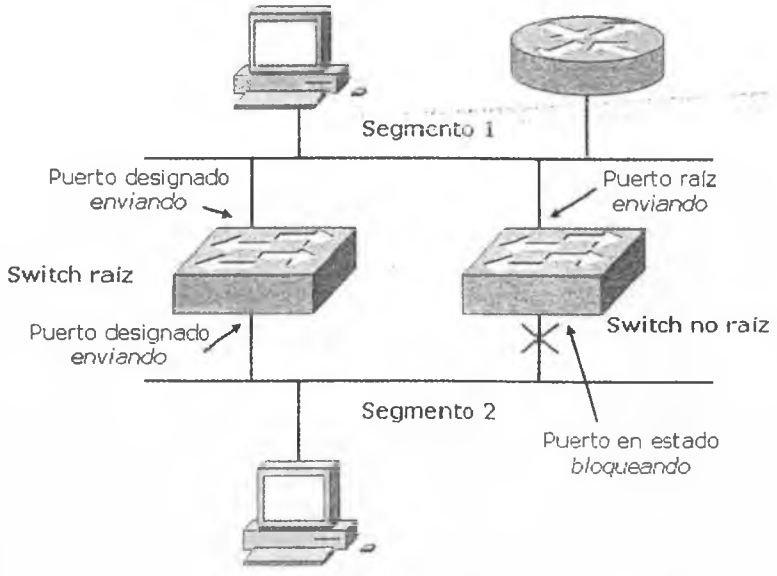
En una red grande pueden convivir en un mismo dominio VTP varios switches servidores trabajando de manera redundante, sin embargo esta alternativa puede dificultar la tarea del administrador.

8.4.2 Estados de los puertos de STP

Los puertos del switch que participan de STP toman diferentes estados según su funcionalidad en la red.

- **Bloqueando**. Inicialmente todos los puertos se encuentran en este estado. Si STP determina que el puerto debe continuar en ese estado, solo escuchará las BPDU pero no las enviará.
- **Escuchando**. En este estado los puertos determinan la mejor topología enviando y recibiendo las BPDU.
- **Aprendiendo**. El puerto comienza a completar su tabla MAC, pero aún no envía tramas. El puerto se prepara para evitar inundaciones innecesarias.
- **Enviando**. El puerto comienza a enviar y recibir tramas.

Existe un quinto estado que es desactivado cuando el puerto se encuentra físicamente desconectado o anulado por el sistema operativo, aunque no es un estado real de STP pues no participa de la operativa STP.



Para evitar bucles, STP bloquea los puertos necesarios

8.5 PROTOCOLO DE ÁRBOL DE EXPANSIÓN RÁPIDO

RSTP es la versión mejorada de STP definido por el estándar IEEE 802.1w. El protocolo de árbol de expansión rápido funciona con los mismos parámetros básicos que su antecesor:

- Designa el switch raíz con las mismas condiciones que STP.
- Elige el puerto raíz del switch no-raíz con las mismas reglas.
- Los puertos designados segmentan la LAN con los mismos criterios.

A pesar de estas similitudes con STP, el modo rápido mejora la convergencia entre los dispositivos ya que STP tarda 50 segundos en pasar del estado bloqueando al enviando mientras que RSTP lo hace prácticamente de inmediato sin necesidad de que los puertos pasen por los otros estados. RSTP es compatible con switches que solo utilicen STP.

En muchos casos el puerto bloqueado es llamado también puerto desechado.

RECUERDE:

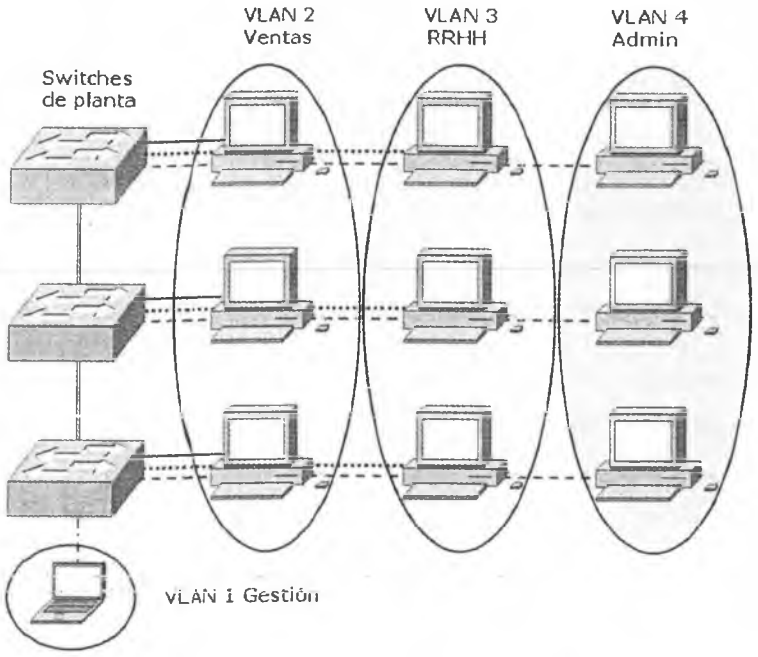
El tiempo que lleva el cambio de estado desde bloqueado a envío es de 50 segundos.

8.6 REDES VIRTUALES

Las VLAN (Lan Virtuales) proveen seguridad, segmentación, flexibilidad, permiten agrupar usuarios de un mismo dominio de broadcast con independencia de su ubicación física en la red. Usando la tecnología VLAN se pueden agrupar lógicamente puertos del switch y los usuarios conectados a ellos en grupos de trabajo con interés común.

Utilizando la electrónica y los medios existentes es posible asociar usuarios lógicamente con total independencia de su ubicación física incluso a través de una WAN. Las VLAN pueden existir en un solo switch o bien abarcar varios de ellos. Las VLAN pueden extenderse a múltiples switch por medio de enlaces troncales que se encargan de transportar tráfico de múltiples VLAN.

El rendimiento de una red se ve ampliamente mejorado al no propagarse las difusiones de un segmento a otro aumentando también los márgenes de seguridad. Para que las VLAN puedan comunicarse son necesarios los servicios de routers que pueden implementar el uso de **ACL** para mantener el margen de seguridad necesario.



Ejemplo de utilización de VLAN

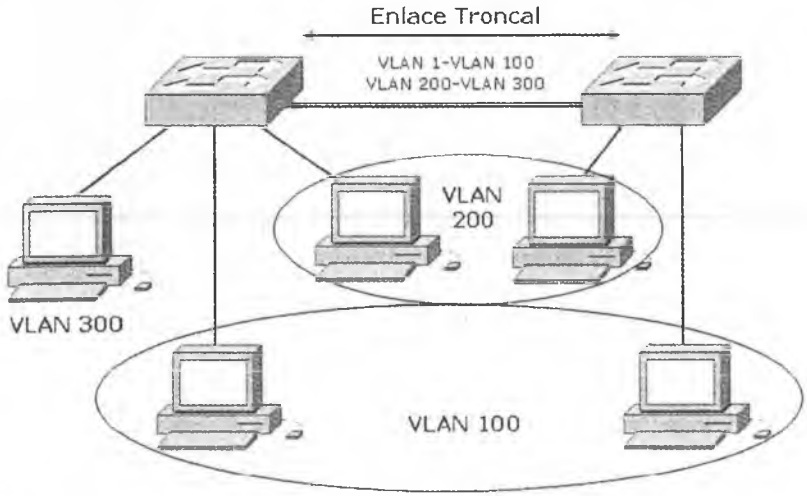
8.7 TRUNKING

Muchas veces es necesario agrupar usuarios de la misma VLAN que se encuentran ubicados en diferentes zonas, para conseguir esta comunicación los switches utilizan un enlace troncal. Para que los switches envíen información sobre las VLAN que tienen configuradas a través de enlaces troncales es necesario que las tramas sean identificadas con el propósito de saber a qué VLAN pertenecen.

A medida que las tramas salen del switch son etiquetadas para indicar a qué VLAN corresponden, esta etiqueta es retirada una vez que entra en el switch de destino para ser enviada al puerto de VLAN correspondiente.

Un puerto de switch que pertenece a una VLAN determinada es llamado **puerto de acceso**, mientras que un puerto que transmite información de varias VLAN a través de un enlace punto a punto es llamado **puerto troncal**.

La información de todas las VLAN creadas viajará por el enlace trocal automáticamente, la VLAN 1, que es la VLAN por defecto o nativa, lleva la información de estado de los puertos. También es la VLAN de gestión.



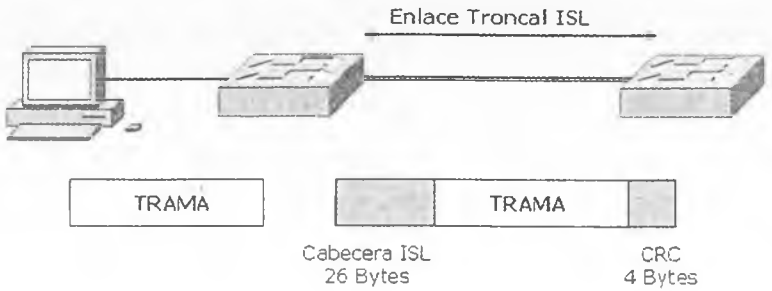
Para evitar que todas las VLAN viajen por el troncal es necesario quitarla manualmente

8.7.1 Etiquetado de trama

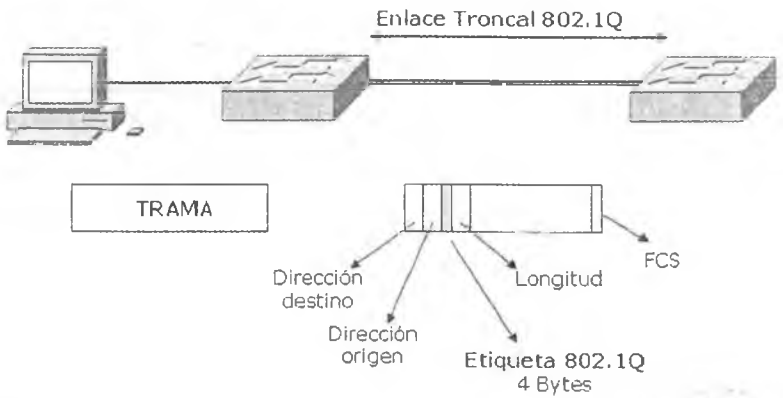
La normativa **IEEE 802.1q** identifica el mecanismo de etiquetado de trama de capa 2 multivendedor. El protocolo **802.1q** interconecta switches, routers y servidores. Solo los puertos FastEthernet y GigabitEthernet soportan el enlace troncal con el etiquetado 802.1q, también conocido como **Dot1q**.

Los switches Cisco implementan una variante de etiquetado propietaria, la ISL (*Inter Switch Link*). ISL funciona a nivel de capa 2 y añade una verificación por redundancia cíclica (CRC). ISL posee muy baja latencia debido a que el etiquetado utiliza tecnología ASIC.

El etiquetado de la trama es eliminado de la trama al salir de un puerto de acceso antes de ser enviada al dispositivo final.



Ejemplo de un etiquetado ISL



Ejemplo de un etiquetado Dot1q

NOTA:

Los switches reconocen la existencia de VLAN a través del etiquetado de trama, identificando el número de VLAN independientemente del nombre que estas posean en cada switch.

8.8 VLAN TRUNKING PROTOCOL

Para conseguir conectividad entre VLAN a través de un enlace troncal entre switches, las VLAN deben estar configuradas en cada switch.

VTP (*Vlan Trunking Protocol*) proporciona un medio sencillo de mantener una configuración de VLAN coherente a través de toda la red conmutada. VTP permite soluciones de red conmutada fácilmente escalable a otras dimensiones, reduciendo la necesidad de configuración manual de la red.

VTP es un protocolo de mensajería de capa 2 que mantiene la misma relación de la configuración VLAN a través de un dominio de administración común, gestionando las adiciones, supresiones y cambios de nombre de las VLAN a través de las redes. Existen varias versiones de VTP; en el caso particular de nuestro enfoque no es fundamental especificar las diferencias entre ellas.

Un dominio VTP son varios switches interconectados que comparten un mismo entorno VTP. Cada switch se configura para residir en un único dominio VTP.

Copia de un **show vtp status**:

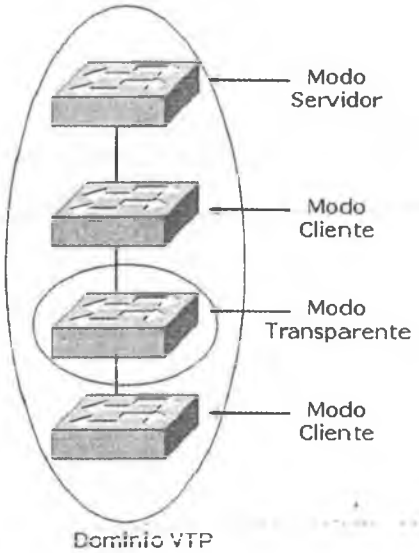
```
switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 63
Maximum VLANs supported locally : 254
Number of existing VLANs        : 20
VTP Operating Mode              : Client
VTP Domain Name                 : damian
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Enabled
MD5 digest                      : 0x38 0x3F 0x5F 0xF0 0x58 0xB6 0x74
0x30
Configuration last modified by 104.10.2.3 at 11-4-06 14:49:55
```

8.9 MODOS DE OPERACIÓN VTP

Cuando se configura VTP es importante elegir el modo adecuado, ya que VTP es una herramienta muy potente y puede crear problemas en la red.

VTP opera en estos tres modos:

- Modo servidor.
- Modo cliente.
- Modo transparente.



En un mismo dominio VTP la información de VLAN configurada en el servidor se transmite a todos los clientes

8.9.1 Modo servidor

El modo VTP predeterminado es el modo servidor. En modo servidor pueden crearse, modificar y suprimir VLAN y otros parámetros de configuración que afectan a todo el dominio VTP. En modo servidor, las configuraciones de VLAN se guardan en la memoria de acceso aleatoria no volátil (NVRAM).

En este modo se envían y retransmiten avisos VTP y se sincroniza la información de configuración de VLAN con otros switches.

RECUERDE:

El modo servidor debe elegirse para el switch que se usará para crear, modificar o suprimir VLAN.

NOTA:

En una red grande pueden convivir en un mismo dominio VTP varios switches servidores trabajando de manera redundante, sin embargo esta alternativa puede dificultar la tarea del administrador.

8.9.2 Modo cliente

Un dispositivo que opera en modo VTP cliente no puede crear, cambiar ni suprimir VLAN.

Un cliente VTP no guarda la configuración VLAN en memoria no volátil. Tanto en modo cliente como en modo servidor, los switches sincronizan su configuración VLAN con la del switch que tenga el número de revisión más alto en el dominio VTP.

En este modo se envían y retransmiten avisos VTP y se sincroniza la información de configuración de VLAN con otros switches.

RECUERDE:

El modo cliente debe configurarse para cualquier switch que se añada al dominio VTP para prevenir un posible reemplazo de configuraciones de VLAN.

8.9.3 Modo transparente

Un switch que opera en VTP transparente no crea avisos VTP ni sincroniza su configuración de VLAN con la información recibida desde otros switches del dominio de administración. Reenvía los avisos VTP recibidos desde otros switches que forman parte del mismo dominio de administración.

Un switch configurado en el modo transparente puede crear, suprimir y modificar VLAN, pero los cambios no se transmiten a otros switches del dominio, afectan tan solo al switch local.

RECUERDE:

El modo transparente debe usarse en un switch que se necesite para avisos VTP a otros switches, pero que necesitan también capacidad para administrar sus VLAN independientemente.

NOTA:

La pertenencia de los puertos de switch a las VLAN se asigna manualmente puerto a puerto (pertenencia VLAN estática o basada en puertos).

8.9.4 Recorte VTP

Por defecto todas las líneas troncales transportan el tráfico de todas las VLAN configuradas. Algún tráfico innecesario podría inundar los enlaces perdiendo efectividad. El recorte o **pruning** VTP permite determinar cuál es el tráfico que inunda el enlace troncal evitando enviarlo a los switches que no tengan configurados puertos de la VLAN destino.

NOTA:

La VLAN1 es la VLAN de administración y se utiliza para tareas de gestión como las publicaciones VTP, no será omitida por el Pruning VTP.

8.10 FUNDAMENTOS PARA EL EXAMEN

- Recuerde y analice los conceptos sobre la microsegmentación y los beneficios de la conmutación de capa 2.
- Recuerde cuáles son los dispositivos que pueden segmentar una LAN y cómo sería el rendimiento de la red con cada uno de ellos.
- Estudie las tecnologías de conmutación, el funcionamiento de cada uno de los métodos.
- Analice el funcionamiento del aprendizaje de direcciones de un switch.
- Razone la problemática que generan los bucles de capa 2.
- Estudie todos los conceptos sobre STP, procesos y estados de los puertos.
- Determine las similitudes y diferencias entre RSTP y STP.
- Recuerde las razones fundamentales para el uso y aplicación de VLAN.
- Analice los beneficios asociados del uso de VLAN.
- Tenga claras las diferencias entre un puerto de acceso y un puerto troncal y para qué utilizaría cada uno.
- Recuerde qué es un enlace troncal y para qué sirve.
- Memorice los tipos de etiquetado de trama, para qué sirven y las diferencias fundamentales entre ambos formatos.
- Memorice y analice el funcionamiento detallado de VTP, sus modos de operación y el recorte VTP.

Capítulo 9

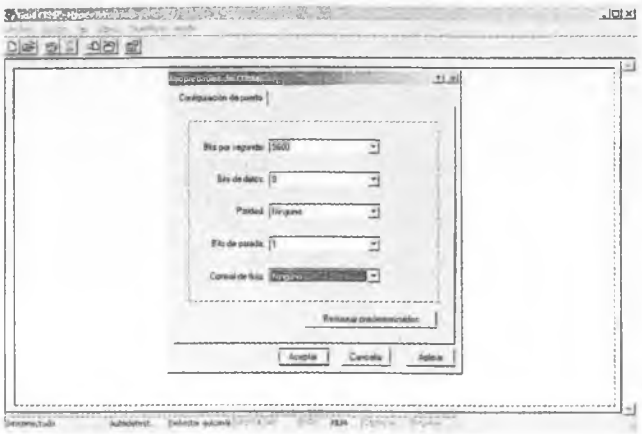
CONGIFIGURACIÓN DEL SWITCH

9.1 CONFIGURACIÓN INICIAL DEL SWITCH

Para la configuración inicial del switch se utiliza el puerto de consola conectado a un cable transpuesto o de consola y un adaptador RJ-45 a DB-9 para conectarse al puerto COM1 del ordenador. Este debe tener instalado un software de emulación de terminal, como el HyperTerminal.

Los parámetros de configuración son los siguientes:

- El puerto COM adecuado.
- 9600 baudios.
- 8 bits de datos.
- Sin paridad.
- 1 bit de parada.
- Sin control de flujo.



La imagen corresponde a una captura de pantalla de HyperTerminal

9.1.1 Asignación de nombre y contraseñas

La asignación de un nombre exclusivo al switch y las contraseñas correspondientes se realiza en el modo de configuración global, mediante los siguientes comandos:

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW_MADRID
SW_MADRID(config)#enable password contraseña
SW_MADRID(config)#enable secret contraseña
SW_MADRID(config)#line console 0
SW_MADRID(config-line)#login
SW_MADRID(config-line)#password contraseña
SW_MADRID(config)#line vty 0 4
SW_MADRID(config-line)#login
SW_MADRID(config-line)#password contraseña
```

9.1.2 Asignación de dirección IP

Para configurar la dirección IP a un switch se debe hacer sobre una interfaz de vlan. Por defecto la VLAN 1 es VLAN nativa del switch, al asignar un direccionamiento a la **interfaz vlan 1** se podrá administrar el dispositivo vía telnet. Si se configura otra interfaz de vlan automáticamente queda anulada la anterior configuración pues solo admite una sola interfaz de vlan.

```
SW_2950(config)#interface vlan 1
SW_2950(config-vlan)#ip address [dirección ip + máscara]
SW_2950(config-vlan)#no shutdown
```

Si el switch necesita enviar información a una red diferente a la de administración se debe configurar un gateway.

```
SW_2950(config)#ip default-gateway[IP de gateway]
```

Para verificar la configuración IP establecida en la VLAN de gestión.

```
SW_2950#show interface vlan 1
```

9.1.3 Guardar y borrar la configuración

Los comandos que permiten hacer copias de seguridad de RAM a NVRAM o TFTP, tanto de la configuración como de la IOS del switch son similares a los descritos para los routers en el Capítulo 3. La siguiente sintaxis muestra cómo copiar de la RAN a la NVRAM y borrarla posteriormente.

```
Switch#copy running-config startup-config

Switch#erase startup-config

Erasing the nvram filesystem will remove all files! Continue?
[confirm]

Erase of nvram: complete
```

RECUERDE:

A pesar de eliminar la configuración de la NVRAM las VLAN no se eliminan debido a que se guardan en un archivo en la memoria flash llamado VLAN.dat.

NOTA:

A pesar de ser un dispositivo antiguo es importante tener en cuenta la asignación de dirección IP en un switch 1900 y el borrado de la configuración de la NVRAM:

```
SW_1900(config)#ip address [dirección ip + máscara]
SW_1900(config)#ip default-gateway[IP de gateway]
SW_1900(config)#delete nvram
```

9.1.4 Configuración de puertos

La configuración básica de puertos se lleva a cabo mediante la determinación de la velocidad y el modo de transmisión. Por defecto, la velocidad asignada es la establecida según el tipo de puerto.

```
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#speed [10 | 100 | auto]
Switch(config-if)#duplex [full | half | auto]
Switch(config-if)#no shutdown
```

Puede verse la **tabla MAC** con las asociaciones de cada puerto con los siguientes comandos:

```
Switch#show mac address-table
Switch#show mac-address-table
```

9.1.5 Seguridad de puertos

El comando **switchport port-security** permite asociar la primera dirección MAC a dicho puerto:

```
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport port-security
```

La cantidad posible de direcciones MAC asociadas al puerto tiene un valor comprendido entre 1 y 132, el comando **switchport port-security maximun** permite establecer la cantidad máxima permitida. El ejemplo ilustra la configuración de un puerto con 10 direcciones MAC máximas posibles.

```
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport port-security maximum 10
```

En el caso de que se detecte algún intento de violación del puerto se puede ejecutar el siguiente comando, haciendo que el puerto quede automáticamente cerrado.

```
Switch(config-if)#switchport port-security violation
[protect|restrict|shutdown]
```

9.2 RECUPERACIÓN DE CONTRASEÑAS

La recuperación de contraseñas le permite alcanzar el control administrativo de su dispositivo si ha perdido u olvidado su contraseña. Para lograr esto necesita conseguir acceso físico a su router, ingresar sin la contraseña, restaurar la configuración y restablecer la contraseña con un valor conocido.

9.2.1 Procedimiento para switches series 2900

Paso 1 - Apague el switch. Vuelva a encenderlo mientras presiona el botón "MODE" (modo) en la parte delantera del switch. Deje de presionar el botón "MODE" una vez que se apaga el LED STAT.

La siguiente información debe aparecer en la pantalla:

```
C2950 Boot Loader (C2950-HBOOT-M) Version 12.1(11r)EA1,
RELEASE
SOFTWARE (fc1)
Compiled Mon 22-Jul-02 18:57 by federtec
WS-C2950-24 starting...
Base ethernet MAC Address: 00:0a:b7:72:2b:40
Xmodem file system is available.

The system has been interrupted prior to initializing the
flash files
system. The following commands will initialize the flash
files system,
and finish loading the operating system software:
flash_init
load_helper
boot
```

Paso 2 - Para inicializar el sistema de archivos y terminar de cargar el sistema operativo, introduzca los siguientes comandos:

```
flash_init
load_helper
dir flash:
```

No se olvide de escribir los dos puntos (:) después de la palabra "flash" en el comando:

```
dir flash:
```

Paso 3 - Escriba **rename flash:config.text flash:config.old** para cambiar el nombre del archivo de configuración. **Este archivo contiene la definición de la contraseña.**

Paso 4 - Escriba **boot** para arrancar el sistema. Responda No a la pregunta:

```
Continue with the configuration dialog? [yes/no]: N
```

Paso 5 - En el indicador del modo EXEC privilegiado, escriba **rename flash:config.old flash:config.text** para cambiar el nombre del archivo de configuración al nombre original.

Paso 6 - Copie el archivo de configuración a la memoria de la siguiente manera:

```
Switch#copy flash:config.text system:running-config
Source filename [config.text]?[enter]
Destination filename [running-config][enter]
```

Paso 7 - Se ha vuelto a cargar el archivo de configuración. Cambie las contraseñas anteriores que se desconocen como se indica a continuación:

```
Switch#configure terminal
Switch(config)#no enable secret
Switch(config)#enable password contraseña nueva
Switch(config)#enable secret contraseña nueva
Switch(config)#line console 0
Switch(config-line)#password contraseña nueva
Switch(config-line)#exit
Switch(config)#line vty 0 15
Switch(config-line)#password contraseña nueva
Switch(config-line)#exit
Switch(config)#exit
Switch#copy running-config startup-config
Destination filename [startup-config]?[enter]
Building configuration...
[OK]
Switch#
```

9.3 CONFIGURACIÓN DE VLAN

Configuración estática. Es la realizada por un administrador creando las VLAN y asignando manualmente los puertos a las respectivas VLAN. Por defecto todos los puertos pertenecen a la VLAN1 hasta que el administrador cambie esta configuración.

Configuración dinámica. El IOS de los switches Catalyst soporta la configuración dinámica a través de un servidor de pertenencia de VLAN (VMPS). El servidor VMPS puede ser un switch de gama alta que ejecute un sistema operativo basado en set (CatOS).

9.3.1 Configuración de VLAN en un switch Catalyst

El proceso de configuración de una VLAN debe seguir los siguientes pasos:

- Crear la VLAN.
- Nombrar la VLAN.
- Asociar uno o más puertos a la VLAN creada.

En la configuración de las VLAN se utiliza un nombre que identificará dicha VLAN, sin embargo el switch solo tiene en cuenta el rango numérico de la misma. El rango de configuración va desde 1 a 1001 y el rango ampliado va de 1006 a 4094. Las VLAN 1 y las 1002 a la 1005 son rangos reservados.

```
Switch(config)# vlan [número de vlan]
Switch(config-vlan)# name nombre de vlan
Switch(vlan)#exit

Switch(config)#interface fastethernet 0/número de puerto
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan [número de vlan]
```

Algunas IOS tambien permiten la configuración con el comando **vlan database**. De la misma manera, el comando **switchport mode access** puede abreviarse simplificando en una sola línea de comandos, **switchport access vlan**.

```
Switch#vlan database
Switch(vlan)#vlan [número de vlan] name nombre de vlan
Switch(vlan)#exit

Switch(config)#interface fastethernet 0/número de puerto
Switch(config-if)#switchport access vlan [número de vlan]
```

RECUERDE:

La VLAN 1 es la llamada VLAN nativa o de administración, que por defecto es a la que se le asigna la dirección IP de gestión del switch.

9.3.2 Configuración de VLAN en un switch 1900

Los switches Catalyst de la serie 1900 prácticamente están en desuso, la siguiente información que se detalla es con carácter informativo. Ejemplo de la creación de una VLAN 6 Administración y su correspondiente asociación al Puerto 0/10:

```
Sw_1900(config)#vlan 6 name administración
Sw_1900(config)#interface ethernet 0/10
Sw_1900(config-if)#vlan-membership static 6
```

El comando **vlan-membership** asocia el puerto estáticamente, con el comando **static**, a la VLAN 6.

Los switches 1900 solo poseen dos puertos FastEthernet, el 26 y el 27. Estos puertos son llamados **A** y **B** respectivamente. Solo admite encapsulación ISL.

```
Sw_1900(config)#interface Fastethernet 0/26
Sw_1900(config-if)#trunk on
Sw_1900(config-if)#exit
Sw_1900(config)#exit

Sw_1900#show trunk A
DISL state:on, Trunking: on, Encapsulation type: ISL
```

9.4 ELIMINACIÓN DE UNA VLAN

En switches de las series 2900 es necesario eliminar el archivo de información de la base de datos de la VLAN que está almacenado en la memoria flash. Tenga especial cuidado de eliminar el archivo VLAN.dat y no otro.

```
Switch#vlan database
Switch(vlan)#no vlan 3
```

El comando para eliminar dicho archivo:

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?[Enter]
Delete flash:vlan.dat? [confirm][Intro]
```

Si no hay ningún archivo VLAN, aparece el siguiente mensaje:

```
%Error deleting flash:vlan.dat (No such file or directory)
```

9.5 HABILITACIÓN DEL ENLACE TRONCAL

Por defecto los puertos troncales trasladan la información de todas la VLAN configuradas, incluso la VLAN 1 que transporta los datos de gestión como por ejemplo VTP.

Existen tres estados de un puerto troncal.

- **on**, por defecto es el estado del puesto troncal (que se recomienda).
- **auto**.
- **desirable**.

```
Switch(config)#interface fastethernet 0/24
Switch(config-if)#switchport mode trunk
```

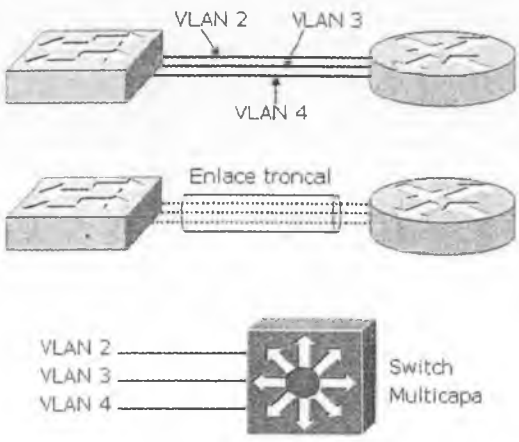
Los switches 2950 solo poseen encapsulación 802.1q, en el caso de ser un switch 2900 se debe especificar la encapsulación deseada:

```
Switch(config)#interface fastethernet 0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk encapsulation [Dot1q|ISL]
```

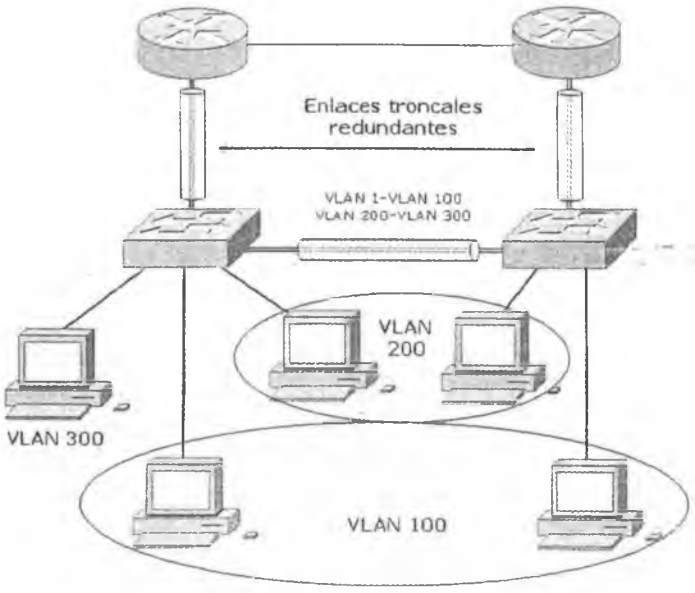
9.6 ENRUTAMIENTO ENTRE VLAN

Para que las VLAN puedan establecer comunicación entre ellas deben ser necesarios los servicios de un router o un switch multicapa. La interconexión puede establecerse directamente a través de interfaces físicas a cada VLAN o con un enlace troncal. Para esto se deben establecer subinterfaces FastEthernet, con su encapsulación y dirección IP correspondiente de manera que cada una de estas subinterfaces pertenezca a un VLAN determinada.

La complementación del filtrado de trama en los switches y las listas de acceso en los routers, hacen que la **seguridad** sea uno de los factores primordiales en el uso de las VLAN.



Enrutamiento entre VLAN con diferentes enlaces



Enrutamiento típico entre VLAN con enlaces troncales redundantes hacia los routers

Los pasos que siguen establecen las configuraciones de una subinterfaz FastEthernet en un router:

```
Router(config)#interface fastethernet [N°de slot/N°de interfaz.N°de
subinterfaz]
Router(config-subif)#encapsulation [dot1q|ISL] [N°de vlan]
```

```
Router(config-subif)#ip address [dirección IP+máscara]
Router(config-subif)#exit
Router(config)#interface fastethernet [N°de slot/N°de interfaz]
Router(config-if)#no shutdown
```

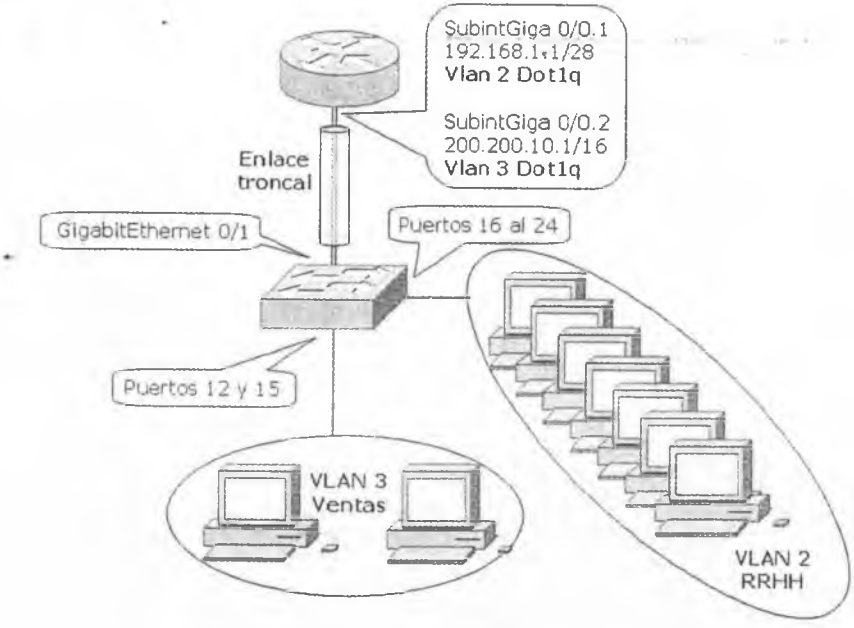
RECUERDE:

Para que la subinterfaz esté "no shutdown" se debe ejecutar este comando directamente desde la interfaz física.

9.7 CASO PRÁCTICO

9.7.1 Configuración de VLAN

Ejemplo de la creación de una VLAN 2 **RRHH** y una VLAN 3 **Ventas** y su asociación a los puertos correspondientes, 12 y 15 **VLAN 3** y los puertos 16 al 24 (configurado por rango) **VLAN 2**.



```
Switch(config)# vlan 3
Switch(config-vlan)# name Ventas
Switch(vlan)#exit
VLAN 3 added:

     Name: Ventas

Switch(vlan)#exit
Switch(config)#interface fastethernet 0/12
Switch(config-if)#switchport access vlan 3
Switch(config)#interface fastethernet 0/15
Switch(config-if)#switchport access vlan 3


Switch(config)# vlan 2
Switch(config-vlan)# name RRHH
Switch(vlan)#exit
VLAN 2 added:

     Name: RRHH

Switch(vlan)#exit
Switch(config)#interface fastethernet 0/16-24
Switch(config-if)#switchport access vlan 2
```

El enlace troncal se realiza a través del puerto GigabitEthernet 0/1, según muestra la sintaxis.

```
Switch(config)#interface GigabitEthernet 0/1
Switch(config-if)#switchport mode trunk
```

9.7.2 Configuración del troncal en el router

Ejemplo de configuración de un enlace troncal sobre dos subinterfaces GigabitEthernet:

```
Router(config)#interface GigabitEthernet 0/0.1
Router(config-subif)#encapsulation dot1q 2
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface GigabitEthernet 0/0.2
Router(config-subif)#encapsulation dot1q 3
Router(config-subif)#ip address 200.200.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#no shutdown
```

9.8 VERIFICACIÓN DE VLAN

En el resumen de la información brindada por un **show vlan** que se muestra a continuación se observa la asociación de las respectivas VLAN, con sus puertos asociados:

```
switch#show vlan
VLAN Name                         Status    Ports
---- ---------------------------- --------- -------------------------------
-
1    default                      active Fa0/1, Fa0/2, Fa0/3, Fa0/4
2    VENTAS                       active Fa0/5, Fa0/6, Fa0/7, Fa0/8,
                                         Fa0/10, Fa0/28, Fa0/30
                                          Fa0/9, Fa0/11, Fa0/12, Fa0/13,
3    ADMINISTRACION               active Fa0/14, Fa0/15, Fa0/16, Fa0/17,
                                         Fa0/18, Fa0/19, Fa0/20, Fa0/21,
4    LOGISTICA                    active Fa0/22, Fa0/23, Fa0/24, Fa0/25,
                                         Fa0/26, Fa0/27, Fa0/29, Fa0/31,
                                         Fa0/32, Fa0/33, Fa0/34, Fa0/35,
                                         Fa0/36, Fa0/37, Fa0/38, Fa0/39,
                                         Fa0/40, Fa0/41, Fa0/42, Fa0/43,
                                         Fa0/44, Fa0/45, Fa0/46, Fa0/47,
                                         Fa0/48
```

- **show vlan brief**. Muestra la información de VLAN resumida.
- **show vtp status**. Muestra la información del estado VTP.
- **show interface trunk**. Muestra los parámetros troncales.
- **show spanning-tree vlan N°**. Muestra información sobre el estado STP.

9.9 CONFIGURACIÓN DE STP

La configuración de STP viene habilitada por defecto. Cisco desarrolló PVST+ para que una red pueda ejecutar una instancia de STP para cada VLAN de la red. La creación de distintos switches raíz en STP por VLAN genera una red más redundante. En ciertos casos será necesaria la configuración de la prioridad, cada switch posee la misma prioridad predeterminada (32768) y la elección del puente raíz para cada VLAN se basará en la dirección MAC. Esta elección en ciertos casos puede no ser la más conveniente.

```
switch(config)#spanning-tree vlan N° priority [0-61440]
```

```
switch(config)#spanning-tree mode ?
  mst         Multiple spanning tree mode
  pvst        Per-Vlan spanning tree mode
  rapid-pvst  Per-Vlan rapid spanning tree mode


switch(config)#interface Fastethernet N°
switch(config-if)#spanning-tree link-type ?
  point-to-point  Consider the interface as point-to-point
  shared          Consider the interface as shared
```

En ciertos casos será necesario desactivar STP aunque se recomienda enfáticamente no deshabilitar STP. En general, STP no es muy exigente para el procesador.

```
switch(config)#no spanning-tree vlan N°
```

En la siguiente captura se observa resaltado la prioridad y más abajo el estado y roll de los puertos

```
switch#show spanning-tree vlan 1

      VLAN0001
        Spanning tree enabled protocol ieee
        Root ID     Priority    8192
                    Address     0003.a0ea.f800
                    Cost        4
                    Port        27 (GigabitEthernet1/0/3)
                    Hello Time   2 sec  Max Age 20 sec  Forward
Delay 15 sec
        Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
                    Address     001b.90b1.8680
                    Hello Time   2 sec  Max Age 20 sec  Forward
Delay 15 sec
                    Aging Time 300

      Interface        Role Sts Cost      Prio.Nbr Type
      ---------------- ---- --- --------- -------- ----
      Gi1/0/3          Root FWD 4         128.27   P2p
      Gi3/0/4          Altn BLK 4         128.132  P2p
```

9.10 CONFIGURACIÓN DE VTP

La configuración de **VTP** comienza determinando cuál será la función de cada switch en la red. Por defecto, los switches vienen configurados en modo

servidor, para cambiar a cualquiera de los otros estados se utiliza el siguiente comando.

```
switch(config)#vtp mode [servidor | cliente | transparente]
```

Se debe determinar un nombre de dominio y una contraseña para este, recuerde que un switch puede participar de diferentes dominios VTP.

```
switch(config)#vtp domain nombre de dominio

switch(config)#vtp password contraseña
```

La siguiente sintaxis de un **show vtp status** muestra la configuración de un switch servidor.

```
switch#show vtp status
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 64
Number of existing VLANs : 5
VTP Operating Mode : Servidor
VTP Domain Name : ccNa
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x8C 0x29 0x40 0xDD 0x7F 0x7A 0x63
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

9.10.1 Guardar y borrar la configuración

Los comandos que permiten hacer copias de seguridad de RAM a NVRAM o TFTP, tanto de la configuración como de la IOS del switch son similares a los descritos para los routers en el Capítulo 3. La siguiente sintaxis muestra cómo copiar de la RAN a la NVRAM y borrarla posteriormente.

```
Switch#copy running-config startup-config

Switch#erase startup-config

Erasing the nvram filesystem will remove all files! Continue?
[confirm]

Erase of nvram: complete
```

tiempo que dure la transmisión. Las sucesivas conexiones pueden o no utilizar la misma ruta que la anterior.

Las conexiones de circuito conmutado suelen emplearse para entornos que tengan uso esporádico, enlaces de respaldo o enlaces bajo demanda. Este tipo de servicios también pueden utilizar los servicios de telefonía básicos mediante una conexión asíncrona conectada a un módem. Un ejemplo es el de RDSI.

- **Paquetes conmutados**. Es un método de conmutación donde los dispositivos comparten un único enlace punto-a-punto o punto-multipunto para transportar paquetes desde un origen hacia un destino a través de una internetwork portadora. Estas redes utilizan circuitos virtuales para ofrecer conectividad, de forma permanente o conmutada (PVC o SVC). El destino es identificado por las cabeceras y el ancho de banda es dedicado, sin embargo una vez entregada la trama el proveedor puede compartirlo con otros clientes. Un ejemplo es el de Frame-Relay.

- **Celdas conmutadas**. Es un método similar al de conmutación de paquetes, solo que en lugar de ser paquetes de longitud variable se utilizan celdas de longitud fija que se transporten sobre circuitos virtuales. Un ejemplo es el de ATM.

10.1.2 Terminología WAN

Los términos y servicios asociados con las tecnologías WAN son cuantiosos, sin embargo los más utilizados son los siguientes:

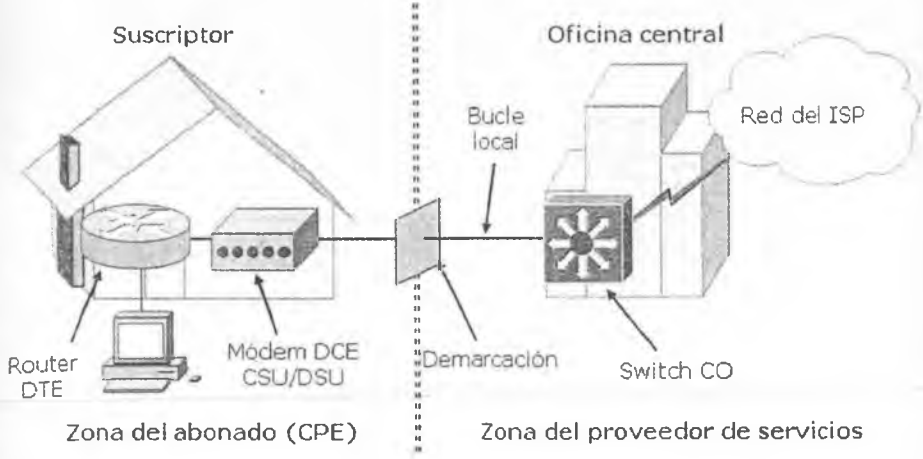
- **CPE** (*Customer Premises Equipment*): dispositivos ubicados físicamente en el cliente.

- **Demarcación**: punto en el que finaliza el CPE y comienza el bucle local.

- **Bucle local**: también llamada última milla, es el cableado desde la demarcación hasta la oficina central del proveedor.

- **CO**: oficina central donde se encuentra el switch CO, dentro de la red pueden existir varios tipos de CO.

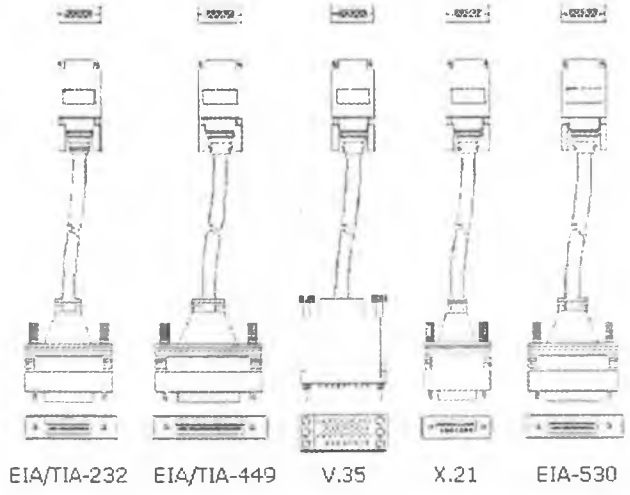
- **Red de Pago**: grupo de dispositivos y recursos que se encuentran dentro de la nube.



Terminología WAN más utilizada

10.1.3 Estándares de línea serie WAN

El siguiente gráfico ilustra los diferentes tipos de conectores para las interfaces serie:



Los dispositivos WAN soportan los siguientes estándares de capa física:

- EIA/TIA-232.
- EIA/TIA-449.
- V.35.
- X.21.
- EIA-530.

NOTA:

La mayoría de los routers utilizan los conectores DB-60, aunque las tarjetas WIC (WAN interface Card) utilizan una interfaz SmartSerial, lo que reduce notablemente el tamaño de las interfaces con las mismas propiedades que las anteriores.

10.1.4 Encapsulación de capa 2 de WAN

Dependiendo de la tecnología WAN utilizada es necesario configurar el tipo de encapsulamiento adecuado.

El siguiente comando en el modo interfaz habilita el encapsulamiento:

```
Router(config-if)#encapsulation [tipo de encapsulación]
```

Entre los tipos de encapsulación WAN se detallan:

- **HDLC** (*High-Level Data Link Control*): es el tipo de encapsulación por defecto de los routers Cisco, es un protocolo de enlace de datos síncrono propietario.
- **PPP** (*Point-to-Point Protocol*): es un protocolo estándar que ofrece conexiones de router a router y de host a red. Utiliza enlaces síncronos y asíncronos. Utiliza mecanismos de autenticación como PAP y CHAP.

- **SLIP** (*Serial Link Internet Protocol*): antecesor de PPP ya casi en desuso.

- **Frame-Relay**: es un protocolo de enlace de datos conmutado y estándar que maneja varios circuitos virtuales para establecer las conexiones. Posee corrección de errores y control de flujo.

- **X.25/ LAPB** (*Link Access Procedure Balanced*): antecesor de Frame-Relay menos fiable que este último.

- **ATM** (*Asynchonous Transfer Mode*): estándar para la transmisión de celdas de longitud fija. Se utiliza indistintamente para voz, vídeo y datos.

10.1.5 Intefaces WAN

Las interfaces seriales WAN responden de forma diferente a las interfaces Ethernet. Es importante poder identificar fallos para resolver posibles incidencias. En muchos casos las interfaces serie tienen errores que no son locales, fallos en las conexiones remotas provocarán caídas inesperadas en dichas interfaces. Los comandos **show interfaces** y **show controllers** brindan soporte logístico para definir errores o conflictos.

```
router>show interfaces serial 0

Serial 0 is up, line protocol is up
Hardware is MCI Serial
Internet address is 131.108.156.98, subnet mask is 255.255.255.240
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load
1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 0:00:00, output 0:00:00, output hang never
Last clearing of "show interface" counters never
Output queue 0/40, 5762 drops; input queue 0/75, 301 drops
Five minute input rate 9000 bits/sec, 16 packets/sec
Five minute output rate 9000 bits/sec, 17 packets/sec
5780806 packets input,785841604 bytes, 0 no buffer
Received 757 broadcasts, 0 runts, 0 giants
146124 input errors, 87243 CRC, 58857 frame, 0 overrun, 0 ignored, 3
abort
5298821 packets output, 765669598 bytes, 0 underruns
0 output errors, 0 collisions, 2941 interface resets, 0 restarts
2 carrier transitions
Interface status line
```

En la sintaxis anterior se resalta el estado de la interfaz, errores en las tramas, paquetes descartados, etc. Las dos sintaxis que siguen corresponden a un router DCE y un router DTE, observe el detalle del sincronismo y tipo de conexión.

```
RouterDCE# sh controllers serial 0/0
Interface Serial0/0
Hardware is PowerQUICC MPC860
DCE V.35, clock rate 56000
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
General [GSMR]=0x2:0x00000000, Protocol-specific [PSMR]=0x8
Events [SCCE]=0x0000, Mask [SCCM]=0x0000, Status [SCCS]=0x00
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E
Interrupt Registers:
Config [CICR]=0x00367F80, Pending [CIPR]=0x0000C000
Mask   [CIMR]=0x00200000, In-srv  [CISR]=0x00000000
Command register [CR]=0x580
Port A [PADIR]=0x1030, [PAPAR]=0xFFFF
       [PAODR]=0x0010, [PADAT]=0xCBFF
Port B [PBDIR]=0x09C0F, [PBPAR]=0x0800E
       [PBODR]=0x00000, [PBDAT]=0x3FFFD
Port C [PCDIR]=0x00C, [PCPAR]=0x200
       [PCSO]=0xC20,  [PCDAT]=0xDF2, [PCINT]=0x00F
Receive Ring
        rmd(68012830): status 9000 length 60C address 3B6DAC4
        rmd(68012838): status B000 length 60C address 3B6D444
Transmit Ring
 --More-

RouterDTE#sh controllers serial 0/0
Interface Serial0/0
Hardware is PowerQUICC MPC860
DTE V.35 TX and RX clocks detected
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
General [GSMR]=0x2:0x00000000, Protocol-specific [PSMR]=0x8
Events [SCCE]=0x0000, Mask [SCCM]=0x0000, Status [SCCS]=0x00
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E
Interrupt Registers:
Config [CICR]=0x00367F80, Pending [CIPR]=0x0000C000
Mask   [CIMR]=0x00200000, In-srv  [CISR]=0x00000000
Command register [CR]=0x580
Port A [PADIR]=0x1030, [PAPAR]=0xFFFF
       [PAODR]=0x0010, [PADAT]=0xCBFF
Port B [PBDIR]=0x09C0F, [PBPAR]=0x0800E
       [PBODR]=0x00000, [PBDAT]=0x3FFFD
Port C [PCDIR]=0x00C, [PCPAR]=0x200
       [PCSO]=0xC20,  [PCDAT]=0xDF2, [PCINT]=0x00F
Receive Ring
        rmd(68012830): status 9000 length 60C address 3B6DAC4
        rmd(68012838): status B000 length 60C address 3B6D444
Transmit Ring
```

RECUERDE:

Las interfaces DCE deben tener configurado el clock rate, es decir el sincronismo o velocidad. Una interfaz local DTE puede presentar fallos si la interfaz remota DCE no tiene correctamente configurado el valor del clock rate. Vea el Capítulo 3. Los keepalive deben ser iguales en ambos extremos.

10.2 PROTOCOLO PUNTO A PUNTO

PPP es un protocolo WAN de enlace de datos. Se diseñó como un protocolo abierto para trabajar con varios protocolos de capa de red, como IP, IPX y Apple Talk.

Se puede considerar a PPP la versión no propietaria de **HDLC**, aunque el protocolo subyacente es considerablemente diferente. PPP funciona tanto con encapsulación síncrona como asíncrona porque el protocolo usa un identificador para denotar el inicio o el final de una trama. Dicho indicador se utiliza en las encapsulaciones asíncronas para señalar el inicio o el final de una trama y se usa como una encapsulación síncrona orientada a bit. Dentro de la trama PPP el bit de entramado es el encargado de señalar el comienzo y el fin de la trama PPP (identificado como 01'11110). El campo de direccionamiento de la trama PPP es un broadcast debido a que PPP no identifica estaciones individuales.

PPP se basa en el protocolo de control de enlaces **LCP** (*Link Control Protocol*), que establece, configura y pone a prueba las conexiones de enlace de datos que utiliza **PPP**. El protocolo de control de red **NCP** (*Network Control Protocol*) es un conjunto de protocolos (uno por cada capa de red compatible con PPP) que establece y configura diferentes capas de red para que funcionen a través de PPP. Para IP, IPX y Apple Talk, las designaciones NCP son IPCP, IPXCP y ATALKCP, respectivamente.

PPP provee mecanismos de control de errores y soporta los siguientes tipos de interfaces físicas:

- Serie síncrona.
- Serie asíncrona.
- RDSI.
- HSSI.

10.2.1 Establecimiento de una conexión PPP

El establecimiento de una sesión PPP tiene tres fases:

1. **Establecimiento del enlace**: en esta fase cada dispositivo PPP envía paquetes LCP para configurar y verificar el enlace de datos.

2. **Autenticación**: fase opcional, una vez establecido el enlace es elegido el método de autenticación. Normalmente los métodos de autenticación son PAP y CHAP.

3. **Protocolo de capa de red**: en esta fase el router envía paquetes NCP para elegir y configurar uno o más protocolos de capa de red. A partir de esta fase los datagramas pueden ser enviados.

10.2.2 Autenticación PAP

PAP (Protocolo de autenticación de contraseña) proporciona un método de autenticación simple utilizando un intercambio de señales de dos vías. El proceso de autenticación solo se realiza durante el establecimiento inicial del enlace.

Autenticación simple con PAP

Una vez completada la fase de establecimiento PPP, el nodo remoto envía repetidas veces al router extremo su usuario y contraseña hasta que se acepta la autenticación o se corta la conexión.

RECUERDE:

PAP no es un método de autenticación seguro, las contraseñas se envían en modo abierto y no existe protección contra el registro de las mismas o los ataques externos.

10.2.3 Configuración de PPP con PAP

Defina el nombre de usuario y la contraseña que espera recibir del router remoto:

```
Router(config)#username[nonbre del remoto] password[contraseña del remoto]
```

Para activar la encapsulación PPP con autenticación PAP en una interfaz se debe cambiar la encapsulación en dicha interfaz serial, el tipo de autenticación y la dirección IP:

```
Router(config-if)#encapsulation PPP
Router(config-if)#ppp authentication pap
Router(config-if)#ip address [dirección IP+máscara]
Router(config-if)#no shutdown
```

Opcionalmente puede configurar la compresión de un software punto a punto en interfaces seriales después de que haya activado la encapsulación PPP.

```
Router(config-if)#compress [predictor | stac]
```

El comando **ppp quality** ***percentage*** garantiza que el enlace satisface los requisitos de calidad que estableció, de lo contrario el enlace se cerraría.

```
Router(config-if)# ppp quality 1-100
```

10.2.4 Autenticación CHAP

CHAP (Protocolo de autenticación por intercambio de señales por desafío) es un método de autenticación más seguro que PAP.

Autenticación por desafío con CHAP

Se emplea durante el establecimiento del enlace y posteriormente se verifica periódicamente para comprobar la identidad del router remoto utilizando señales de tres vías. La contraseña es encriptada utilizando MD5, una vez establecido el enlace el router agrega un mensaje desafío que es verificado por ambos routers, si ambos coinciden, se acepta la autenticación, de lo contrario la conexión se cierra inmediatamente.

RECUERDE:

CHAP ofrece protección contra ataques externos mediante el uso de un valor de desafío variable que es único e indescifrable. Esta repetición de desafíos limita la posibilidad de ataques.

10.2.5 Configuración de PPP con CHAP

Defina el nombre de usuario y la contraseña que espera recibir del router remoto:

```
Router(config)#username nonbre del remoto password contraseña
```

Puede usar el mismo nombre de host en múltiples routers cuando quiera que el router remoto crea que está conectado a un solo router.

Para activar la encapsulación PPP con autenticación CHAP en una interfaz se debe cambiar la encapsulación en dicha interfaz serial, el tipo de autenticación, el nombre con el que el router remoto reconocerá el local, la contraseña con la que hará el desafío el router local y la dirección IP:

```
Router(config-if)#encapsulation PPP
Router(config-if)#ppp authentication chap
Router(config-if)#ip address [dirección IP+máscara]
Router(config-if)#no shutdown
```

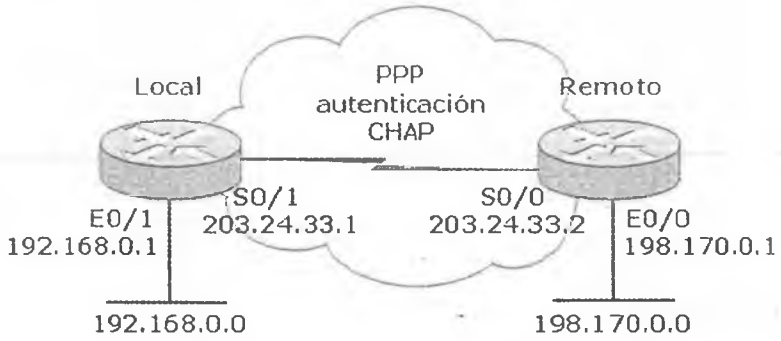
Para autenticarse frente a un host desconocido debe configurar en la interfaz correspondiente la contraseña que será enviada a los hosts que quieran autenticar al router. También sirve para limitar la cantidad de entradas en el router.

```
Router(config-if)#ppp chap password contraseña
```

10.3 CASO PRÁCTICO

10.3.1 Configuración PPP con autenticación CHAP

Las siguientes sintaxis muestran las configuraciones básicas de una conexión serie punto a punto utilizando una encapsulación PPP y una autenticación CHAP:



Router Local:

```
Router(config)#hostname Local
Local(config)#username Remoto password cisco
Local(config)#interface serial 0/1
Local(config-if)#encapsulation PPP
Local(config-if)#ppp authentication chap
Local(config-if)#ip address 203.24.33.1 255.255.255.0
Local(config-if)#no shutdown
Local(config-if)#exit
Local(config)#interface ethernet 0/1
Local(config-if)#ip address 192.168.0.1 255.255.255.0
Local(config-if)#no shutdown
Local(config-if)#exit
Local(config)#router ospf 100
Local(config-router)#network 192.168.0.0 0.0.0.255 area 0
Local(config-router)#network 203.24.33.0 0.0.0.255 area 0
```

Router Remoto:

```
Router(config)#hostname Remoto
Remoto(config)#username Local password cisco
Remoto(config)#interface serial 0/0
Remoto(config-if)#clockrate 56000
```

```
Remoto(config-if)#encapsulation PPP
Remoto(config-if)#ppp authentication chap
Remoto(config-if)#ip address 203.24.33.2 255.255.255.0
Remoto(config-if)#no shutdown
Remoto(config)#interface ethernet 0/0
Remoto(config-if)#ip address 198.170.0.1 255.255.255.0
Remoto(config-if)#no shutdown
Remoto(config-if)#exit
Remoto(config)#router ospf 100
Remoto(config-router)#network 198.170.0.0 0.0.0.255 area 0
Remoto(config-router)#network 203.24.33.0 0.0.0.255 area 0
```

10.3.2 Verificación PPP

- **show interfaces**. Muestra el estado de las interfaces con su autenticación.

- **debug ppp authentication**. Muestra el proceso de autenticación.

```
Router1#show int bri0/0
BRI0 is standby mode, line protocol is down
  Hardware is BRI
  Internet address is 10.1.99.55/24
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/16 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 48 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 7 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

10.4 TRADUCCIÓN DE DIRECCIONES DE RED

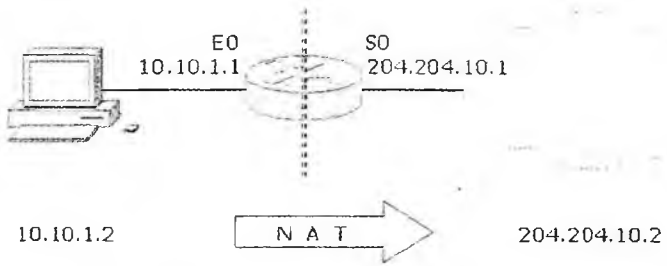
NAT (*Network Address Traslation*) permite acceder a Internet traduciendo las direcciones privadas en direcciones IP registradas. Incrementa la seguridad y la privacidad de la red local al traducir el direccionamiento interno a uno externo.

NAT tiene varias formas de trabajar según los requisitos y la flexibilidad de que se disponga, cualquiera de ellas es sumamente importante a la hora de controlar el tráfico hacia el exterior:

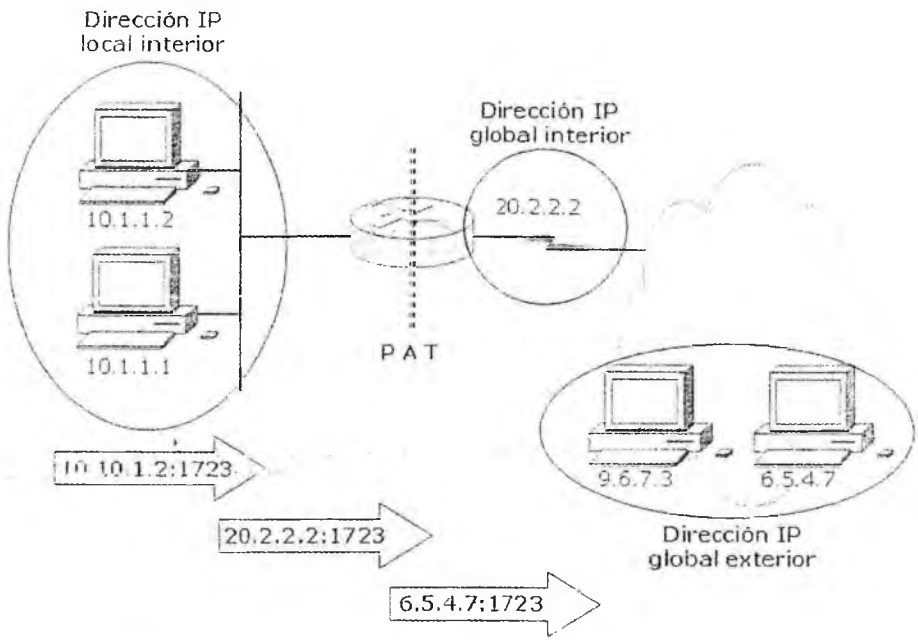
- **Estáticamente**: NAT permite la asignación de una a una entre las direcciones locales y las exteriores o globales.
- **Dinámicamente**: NAT permite asignar a una red IP interna a varias externas incluidas en un grupo o pool de direcciones.
- **PAT** (*Port Address Traslation*): es una forma de NAT dinámica, comúnmente llamada NAT sobrecargado, que asigna varias direcciones IP internas a una sola externa. PAT utiliza números de puertos de origen únicos en la dirección global interna para distinguir entre las diferentes traducciones.

10.4.1 Terminología NAT

- **Dirección local interna**: es la dirección IP asignada a un host de la red interna.
- **Dirección global interna**: es la dirección IP asignada por el proveedor de servicio que representa a la dirección local ante el mundo.
- **Dirección local externa**: es la dirección IP de un host externo tal como lo ve la red interna.
- **Dirección global externa**: es una dirección IP asignada por el propietario a un host de la red externa.



Traducción de una dirección de red estáticamente



PAT utiliza números de puertos de origen únicos en la dirección global interna para distinguir entre las diferentes traducciones

10.4.2 Configuración de NAT estático

Para configurar NAT estáticamente utilice el siguiente comando:

```
Router(config)#ip nat inside source static [ip interna][ip externa]
```

Defina cuáles serán las interfaces de entrada y salida y su correspondiente dirección IP:

```
Router(config)#interface [tipo][número]
Router(config-if)#ip address [ip de la interfaz interna+máscara]
Router(config-if)#ip nat inside
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)# interface [tipo][número]
Router(config-if)#ip address [ip de la interfaz externa+máscara]
Router(config-if)#ip nat outside
Router(config-if)#no shutdown
Router(config-if)#exit
```

10.4.3 Configuración de NAT dinámico

Para configurar NAT dinámicamente se debe crear un pool de direcciones, para ello utilice el siguiente comando:

```
Router(config)#ip nat pool nombre del pool[ip inicio][ip final]
netmask[máscara]
```

Defina una lista de acceso que permita solo a las direcciones que deban traducirse:

```
Router(config)#acces-list 1 permit [ip interna permitida][wildcard]
```

Asocie la lista de acceso al pool:

```
Router(config)#ip nat inside source list 1 pool nombre del pool
```

Defina las interfaces de entrada y salida:

```
Router(config)#interface [tipo][número]
Router(config-if)#ip address [ip de la interfaz interna+máscara]
Router(config-if)#ip nat inside
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)# interface [tipo][número]
Router(config-if)#ip address [ip de la interfaz externa+máscara]
Router(config-if)#ip nat outside
Router(config-if)#no shutdown
Router(config-if)#exit
```

10.4.4 Configuración de PAT

PAT o **NAT sobrecargado** se configura definiendo una lista de acceso que permita solo a las direcciones que deban traducirse:

```
Router(config)#access-list 1 permit [ip interna permitida] [wildcard]
```

Asocie dicha lista a la interfaz de salida agregando al final el comando **overload**:

```
Router(config)#ip nat inside source list 1 interface [tipo] [número]
overload
```

Defina las interfaces de entrada y salida:

```
Router(config)#interface [tipo] [número]
Router(config-if)#ip address [ip de la interfaz interna+máscara]
Router(config-if)#ip nat inside
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)# interface [tipo] [número]
Router(config-if)#ip address [ip de la interfaz externa+máscara]
Router(config-if)#ip nat outside
Router(config-if)#no shutdown
Router(config-if)#exit
```

10.5 CASO PRÁCTICO

10.5.1 Configuración dinámica de NAT

El ejemplo muestra la configuración de un router con NAT dinámico donde se ha creado un pool de direcciones IP llamado INTERNET, la interfaz entrante es la ethernet 0/0 y la saliente la serial 0/1:

```
Router(config)#ip nat INTERNET 204.204.10.20 204.204.10.30 netmask
255.255.255.0
Router(config)#acces-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#ip nat inside source list 1 pool INTERNET
Router(config)#interface ethernet 0/0
Router(config-if)#ip address 192.168.1.25 255.255.255.0
Router(config-if)#ip nat inside
Router(config-if)#no shutdown
```

```
Router(config-if)#exit
Router(config)# interface serial 0/1
Router(config-if)#ip address 204.204.20.11 255.255.255.0
Router(config-if)#ip nat outside
Router(config-if)#no shutdown
Router(config-if)#exit
```

10.5.2 Verificación NAT

- **Show ip nat traslations**. Muestra las traslaciones de direcciones IP.
- **Show ip nat statistics**. Muestra las estadísticas NAT.
- **Debug ip nat**. Muestra los procesos de traslación de dirección.

```
Router# show ip nat translations

Pro Inside global     Inside local    Outside local  Outside global

--- 171.16.233.209    192.168.1.95    ---            ---
--- 171.16.233.210    192.168.1.89    ---            ---


Router# show ip nat statistics

Total translations: 2 (0 static, 2 dynamic; 0 extended)
Outside interfaces: Serial0
Inside interfaces: Ethernet1
Hits: 135  Misses: 5
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool net-208 refcount 2
 pool net-208: netmask 255.255.255.240
    start 172.16.233.208 end 172.16.233.221
    type generic, total addresses 14, allocated 2 (14%), misses 0
```

RECUERDE:

Las listas de acceso asociadas a NAT deben permitir solo el acceso a las redes que se van a convertir, sea específico y no utilice el permit any.

10.6 FRAME-RELAY

Frame-Relay define el proceso para enviar datos sobre la red pública de datos, constituye una tecnología de enlace de datos orientada a la conexión de alto rendimiento y eficacia. Frame-Relay delega en los protocolos de las capas superiores la corrección de errores (TCP).

Es un protocolo basado en estándares de capa uno y dos del modelo de referencia OSI. Define la conexión entre la red de un proveedor de servicio y el dispositivo de un usuario.

Los dispositivos Frame-Relay se dividen en dos grupos:

- **DTE** (*Data Terminal Equipment*): equipo del cliente que finaliza la conexión Frame-Relay.
- **DCE** (*Data Circuit-Terminating Equipment*): son los dispositivos de red propiedad del proveedor.

10.6.1 Terminología Frame-Relay

- **PVC**. Circuito virtual permanente. Circuito virtual que se establece de forma permanente. Los PVC permiten ahorrar ancho de banda asociado con el establecimiento y corte de circuitos si determinados circuitos virtuales deben existir en todo momento.
- **SVC**. Circuito virtual conmutado. Circuito virtual que se establece de forma dinámica a pedido y que se interrumpe cuando la transmisión se completa. Los SVC se utilizan cuando la transmisión de datos es esporádica.
- **DLCI**. Identificador de conexión de enlace de datos. Valor que especifica un PVC o SVC en una red Frame-Relay. En la especificación Frame-Relay básica, los DLCI son significativos a nivel local (los dispositivos conectados pueden usar distintos valores para especificar la misma conexión). En la especificación LMI extendida, los DLCI son significativos a nivel global (los DLCI especifican dispositivos finales individuales).
- **CIR**. Velocidad de información suscrita. Velocidad a la cual una red Frame-Relay acepta transferir información en condiciones normales, con un promedio sobre un incremento de tiempo mínimo. La CIR, que

se mide en bits por segundo, es una de las métricas clave del tráfico negociado.

- **ARP inverso**. Protocolo de resolución de direcciones inverso. Método para crear rutas dinámicas en una red. Permite que un dispositivo detecte la dirección de red de otro asociado a través de un circuito virtual.

- **LMI**. Interfaz de administración local. Conjunto de mejoras para la especificación Frame-Relay básica. La LMI incluye soporte para un mecanismo de mensajes de actividad, que verifica que los datos fluyan; un mecanismo de multicast, que proporciona al servidor de red su DLCI local y el DLCI multicast; direccionamiento global, que proporciona a los DLCI significado global en lugar de simplemente significado local en la red Frame-Relay; y un mecanismo de estado, que indica el estado en curso en los DLCI que el switch conoce.

- **FECN**. Notificación explícita de congestión. Bit establecido por una red Frame-Relay para informar al DTE que recibe la trama de que se ha experimentado congestión en la ruta desde el origen hacia el destino. Los DTE que reciben tramas con el bit FECN establecido pueden solicitar que los protocolos de mayor nivel tomen las acciones de control de flujo que sean necesarias.

- **BECN**. Notificación retrospectiva de congestión en la red. Bit establecido por una red Frame-Relay en las tramas que viajan en dirección opuesta a las tramas que encuentran una ruta congestionada. Los DTE que reciben tramas con el bit BECN ya establecido pueden solicitar que los protocolos de mayor nivel tomen las acciones de control de flujo que sean necesarias.

10.6.2 Topologías Frame-Relay

Una de las cuestiones más útiles que ofrece Frame-Relay es la flexibilidad de conexión hacia la nube Frame-Relay. El proveedor ofrece circuitos virtuales capaces de interconectar los sitios remotos con una topología particular.

- **Topología de malla completa**. Todos los routers disponen de circuitos virtuales al resto de los destinos.

- **Topología de malla parcial**. Es un tipo de malla completa pero no todos los sitios tienen acceso a los demás.

- **Topología en estrella**. Los sitios remotos están conectados a un punto central que por lo general ofrece un servicio o una aplicación.

RECUERDE:

Frame-Relay utiliza horizonte dividido para evitar bucles de enrutamiento.

10.6.3 Funcionamiento de Frame-Relay

Cada circuito virtual está identificado de forma única por un **DLCI local**, lo que permite distinguir qué router está conectado a cada interfaz. Es posible configurar manualmente una asignación estática en la tabla de asignaciones del router para poder describir la relación entre el circuito virtual y la dirección de capa 3 del otro extremo.

Las direcciones pueden asignarse también de forma dinámica mediante **ARP inverso** que asocia un DLCI con la dirección del siguiente salto. Las LMI son responsables de la administración y el mantenimiento del estado de enlace de los dispositivos. Los LMI son configurables, aunque las versiones actuales de IOS las detectan automáticamente.

Existen tres tipos de LMI:

- **Cisco**. por defecto definidas para equipos Cisco.
- **ANSI**.
- **Q933a**.

Para iniciar el proceso de comunicación se deben producir los siguientes pasos:

1. Cada router es conectado al switch Frame-Relay por medio de un CSU/DSU.
2. El router indaga el estado del circuito virtual.
3. Cuando el switch Frame-Relay recibe la petición responde informando los DLCI locales de los PVC a los routers remotos.

4. Por cada DLCI activo los routers envían un paquete ARP inverso que contiene la dirección IP correspondiente a cada circuito virtual.

5. Los routers remotos crean tablas que incluyen los DLCI locales y las direcciones IP.

6. Cada 60 segundos se envían los mensajes ARP inverso.

7. Cada 10 segundos se intercambia información LMI.

Dentro de la nube Frame-Relay el switch crea tablas con la relación que tienen cada puerto/slot con los DLCI de los routers remotos.

10.6.4 Configuración básica de Frame-Relay

El primer paso dentro de la configuración de Frame-Relay es el de la activación de la interfaz que conecta a dicho router con una CSU/DSU, conectada a su vez con el switch del proveedor.

Además de la dirección IP correspondiente se debe establecer el tipo de encapsulación:

- **IETF** para equipos no Cisco.
- **Cisco** para equipos Cisco, en el caso de elegir esta encapsulación no hará falta especificarla.

```
Router(config)#interface Serial 1
Router(config-if)#ip address [direction IP+máscara]
Router(config-if)#encapsulation frame-relay [cisco/ietf]
Router(config-if)#bandwidth [valor del ancho de banda en Kbps]
```

Si fuera necesario, según la versión de IOS, configurar LMI:

```
Router(config-if)#frame-relay lmi-type [cisco/anci/q933a]
```

ARP inverso está activado por defecto, si fuera necesario activarlo:

```
Router(config-if)#frame-relay inverse-arp [protocolo] [dlci]
```

Donde:

- **protocolo**: IP, IPX, appletalk, decnet, etc.
- **dlci**: número de dlci de la interfaz local, valor entre el 16 y 1007.

10.6.5 Configuración estática de Frame-Relay

Cuando un router no soporta **ARP inverso**, o cuando se quiere controlar el tráfico sobre los circuitos virtuales, se debe definir estáticamente una tabla de dirección remota y su DLCI.

A partir de la configuración básica se agrega el mapeo estático:

```
Router(config-if)#frame-relay map [protocolo] [dirección
destino] [DLCI local] [broadcast] [ietf/cisco] [payload-compress paket-
by-paket]
```

Donde se define el tipo de protocolo, la dirección IP del destino y el DLCI local. Con dispositivos Cisco no es necesaria la configuración de la encapsulación, mientras que con dispositivos no Cisco se debe utilizar IETF. Los parámetros restantes son opcionales y habilitan el envío de difusiones y la compresión de sobrecarga.

10.6.6 Configuración de las subinterfaces Frame-Relay

Al establecer una conexión con un CSU/DSU se pueden abastecer varios PVC en una sola conexión física. Para este fin es necesario configurar subinterfaces que actúen como interfaces lógicas conectadas a los PVC.

Una subinterfaz no tiene forma predeterminada de conexión y puede configurase como:

- **Punto a punto**: cada subinterfaz establece una conexión PVC directa punto a punto con su correspondiente router remoto. El tráfico de actualización de enrutamiento NO está sujeto a la regla del horizonte dividido.
- **Multipunto**: una subinterfaz establece múltiples conexiones PVC a través de la nube Frame-Relay a varias interfaces físicas o subinterfaces de los routers remotos. El tráfico de actualización de enrutamiento está sujeto a la regla del horizonte dividido.

Proceso de configuración de subinterfaces.

- Seleccione la interfaz en la que creará las subinterfaces y verifique la no existencia de direccionamiento de capa tres (este paso es fundamental). Si tiene dudas ejecute un **no ip address** sobre la interfaz.
- Configure la encapsulación Frame-Relay correspondiente en dicha interfaz.
- Seleccione la subinterfaz y si se utilizará como punto a punto o multipunto, rango de 0-4.294.967.295. Recuerde que no tienen valor predeterminado.
- Configure el valor de DLCI local en la subinterfaz, rango de 16-1007.

La siguiente sintaxis describe la configuración de las subinterfaces Frame-Relay.

```
Router(config)#interface Serial [número]
Router(config-if)#no ip address
Router(config-if)#encapsulation frame-relay
Router(config-if)#exit
Router(config)#interface serial [número.número de
subinterfaz] [multipoint/point-to-point]
Router(config-subif)#frame-relay interface-dlci [DLCI local]
```

10.7 CASO PRÁCTICO

10.7.1 Configuración estática de Frame-Relay

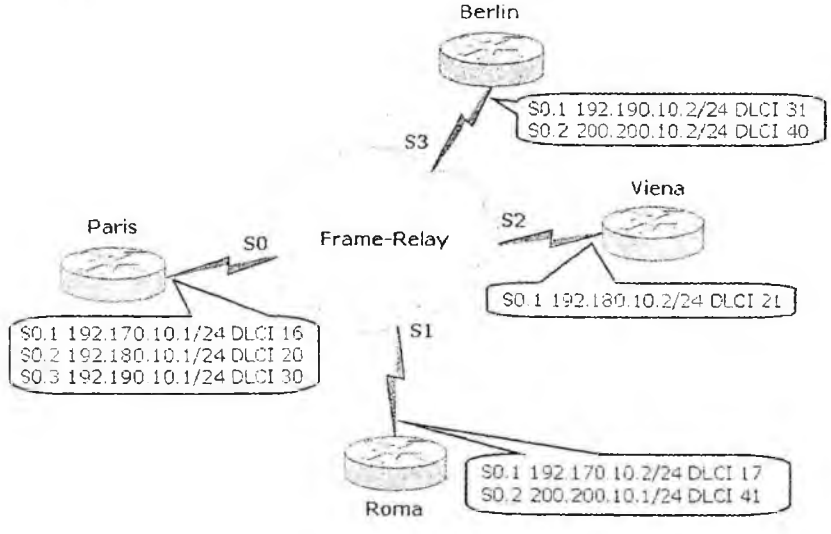
La siguiente topología muestra una conexión simple Frame-Relay punto a punto.


```
ORIGEN(config)#interface Serial 1
ORIGEN(config-if)#ip address 10.16.0.1 255.255.255.0
ORIGEN(config-if)#encapsulation frame-relay
ORIGEN(config-if)#bandwidth 64
ORIGEN(config-if)#frame-relay map ip 10.16.0.2 110 broadcast

REMOTO(config)#interface Serial 2
REMOTO(config-if)#ip address 10.16.0.2 255.255.255.0
REMOTO(config-if)#encapsulation frame-relay
REMOTO(config-if)#bandwidth 64
REMOTO(config-if)#frame-relay map ip 10.16.0.1 100 broadcast
```

10.7.2 Configuración de una nube Frame-Relay

La siguiente topología muestra una nube Frame-Relay con conexiones multipunto.



Router	Tipo de interfaz	Dirección IP	DLCI	Interfaz remota
Paris	Serial 0.1	192.170.10.1/24	16	Serial 0.1 Roma
Paris	Serial 0.2	192.180.10.1/24	20	Serial 0.1 Viena
Paris	Serial 0.3	192.190.10.1/24	30	Serial 0.1 Berlin
Berlin	Serial 0.1	192.190.10.2/24	31	Serial 0.3 Paris
Berlin	Serial 0.2	200.200.10.2/24	40	Serial 0.2 Roma
Viena	Serial 0.1	192.180.10.2/24	21	Serial 0.2 Paris
Roma	Serial 0.1	192.170.10.2/24	17	Serial 0.1 Paris
Roma	Serial 0.2	200.200.10.3/24	41	Serial 0.2 Berlin

Configuración routers remotos:

```
Paris#config t
Paris(config)#interface Serial 0
Paris(config-if)#no ip address
Paris(config-if)#encapsulation frame-relay
Paris(config-if)#no shutdown
Paris(config-if)#exit
Paris(config)# interface serial 0.1 multipoint
Paris(config-subif)#ip address 192.170.10.1 255.255.255.0
Paris(config-subif)#description CONEXION A ROMA
Paris(config-subif)#Frame-relay interface-dlci 16
Paris(config-subif)#exit
Paris(config)# interface serial 0.2 multipoint
Paris(config-subif)#ip address 192.180.10.1 255.255.255.0
Paris(config-subif)#description CONEXION A VIENA
Paris(config-subif)#Frame-relay interface-dlci 20
Paris(config-subif)#exit
Paris(config)# interface serial 0.3 multipoint
Paris(config-subif)#ip address 192.190.10.1 255.255.255.0
Paris(config-subif)#description CONEXION A BERLIN
Paris(config-subif)#Frame-relay interface-dlci 30
Paris(config-subif)#exit
Paris(config)# router rip
Paris(config-router)#network 192.170.10.0
Paris(config-router)#network 192.180.10.0
Paris(config-router)#network 192.190.10.0
```

```
Berlin#config t
Berlin(config)#interface Serial 0
Berlin config-if)#no ip address
Berlin(config-if)#encapsulation frame-relay
Berlin(config-if)#no shutdown
Berlin(config-if)#exit
Berlin(config)#interface serial 0.1 multipoint
Berlin(config-subif)#ip address 192.190.10.2 255.255.255.0
Berlin(config-subif)#description CONEXION A PARIS
Berlin(config-subif)#Frame-relay interface-dlci 31
Berlin(config-subif)#exit
Berlin(config)#interface serial 0.2 multipoint
Berlin(config-subif)#ip address 220.200.10.2 255.255.255.0
Berlin(config-subif)#description CONEXION A ROMA
Berlin(config-subif)#Frame-relay interface-dlci 40
Berlin(config-subif)#exit
Berlin(config)#router rip
Berlin(config-router)#network 220.200.10.0
Berlin(config-router)#network 192.190.10.0

Viena#config t
Viena(config)#interface Serial 0
Viena(config-if)#no ip address
Viena(config-if)#encapsulation frame-relay
Viena(config-if)#no shutdown
Viena(config-if)#exit
Viena(config)#interface serial 0.1 multipoint
Viena(config-subif)#ip address 192.180.10.2 255.255.255.0
Viena(config-subif)#description CONEXION A PARIS
Viena(config-subif)#Frame-relay interface-dlci 21
Viena(config-subif)#exit
Viena(config)#router rip
Viena(config-router)#network 192.180.10.0

Roma#config t
Roma(config)# interface Serial 0
Roma(config-if)# no ip address
Roma(config-if)# encapsulation frame-relay
Roma(config-if)# no shutdown
Roma(config-if)#exit
Roma(config)# interface serial 0.1 multipoint
Roma(config-subif)# ip address 192.170.10.2 255.255.255.0
Roma(config-subif)#description CONEXION A PARIS
Roma(config-subif)#Frame-relay interface-dlci 17
Roma(config-subif)#exit
Roma(config)# interface serial 0.2 multipoint
Roma(config-subif)# ip address 220.200.10.3 255.255.255.0
Roma(config-subif)#description CONEXION A BERLIN
Roma(config-subif)#Frame-relay interface-dlci 41
Roma(config-subif)#exit
Roma(config)# router rip
Roma(config-router)# network 220.200.10.0
Roma(config-router)# network 192.170.10.0
```

Configuración de switch Frame-Relay:

```
frame-relay(config)# frame-relay switching
```

*** Configurar Interfaz S0 Conectada directamente con París ***

```
frame-relay(config)# interface Serial0
frame-relay(config-if)# no ip address
frame-relay(config-if)# encapsulation frame-relay
frame-relay(config-if)#description CONEXION A PARIS
frame-relay(config-if)# clock rate 56000
frame-relay(config-if)# frame-relay intf-type dce
frame-relay(config-if)# frame-relay route 16 interface serial 1 17
frame-relay(config-if)# frame-relay route 20 interface serial 2 21
frame-relay(config-if)# frame-relay route 30 interface serial 3 31
frame-relay(config-if)# no shutdown
```

*** Configurar Interfaz S1 Conectada directamente con Roma ***

```
frame-relay(config)# interface Serial1
frame-relay(config-if)# no ip address
frame-relay(config-if)# encapsulation frame-relay
frame-relay(config-if)#description CONEXION A ROMA
frame-relay(config-if)# clock rate 56000
frame-relay(config-if)# frame-relay intf-type dce
frame-relay(config-if)# frame-relay route 17 interface serial 0 16
frame-relay(config-if)# frame-relay route 41 interface serial 3 40
frame-relay(config-if)# no shutdown
```

*** Configurar Interfaz S2 Conectada directamente con Viena ***

```
frame-relay(config)# interface Serial2
frame-relay(config-if)# no ip address
frame-relay(config-if)# encapsulation frame-relay
frame-relay(config-if)#description CONEXION A VIENA
frame-relay(config-if)# clock rate 56000
frame-relay(config-if)# frame-relay intf-type dce
frame-relay(config-if)# frame-relay route 21 interface serial 0 20
frame-relay(config-if)# no shutdown
```

*** Configurar Interfaz S3 Conectada directamente con Berlín ***

```
frame-relay(config)# interface Serial3
frame-relay(config-if)# no ip address
frame-relay(config-if)# encapsulation frame-relay
frame-relay(config-if)#description CONEXION A BERLIN
frame-relay(config-if)# clock rate 56000
```

```
frame-relay(config-if)# frame-relay intf-type dce
frame-relay(config-if)# frame-relay route 31 interface serial 0 30
frame-relay(config-if)# frame-relay route 40 interface serial 1 41
frame-relay(config-if)# no shutdown
frame-relay#show frame-relay route
```

10.7.3 Verificación Frame-Relay

- **Show interfaces**. Muestra el estado de la conexión Frame-Relay.
- **Show frame-relay lmi**. Muestra las estadísticas de tráfico LMI.
- **Show frame-relay pvc**. Muestra la conexión y las estadísticas de tráfico, BECN, FECN, DLCI, etc.
- **Show frame-relay map**. Muestra la información contenida en los mapas, como por ejemplo IP mapeadas a las DLCI.
- **Debug frame-relay lmi**. Verifica si se envían y reciben paquetes LMI.

```
router# show frame-relay pvc 16

PVC Statistics for interface POS5/0 (Frame Relay NNI)

DLCI = 16, DLCI USAGE = SWITCHED, PVC STATUS = INACTIVE, INTERFACE =
POS5/0
LOCAL PVC STATUS = INACTIVE, NNI PVC STATUS = ACTIVE

  input pkts 0              output pkts 0             in bytes 0
  out bytes 0               dropped pkts 100          in FECN pkts 0
  in BECN pkts 0            out FECN pkts 0           out BECN pkts 0
  in DE pkts 0              out DE pkts 0
  out bcast pkts 0          out bcast bytes 0
  switched pkts 0
  Detailed packet drop counters:
  no out intf 0             out intf down 100         no out PVC 0
  in PVC down 0             out PVC down 0            pkt too big 0
  pvc create time 00:25:32, last time pvc status changed 00:06:31

Router# show frame-relay map

Serial 1 (administratively down): ip 131.108.177.177
dlci 177 (0xB1,0x2C10), static,
broadcast,
CISCO
TCP/IP Header Compression (inherited), passive (inherited)
```

10.8 INTRODUCCIÓN A VPN

Una VPN (Red Privada Virtual) se utiliza principalmente para conectar dos redes privadas a través de la red pública de datos. Sin embargo puede tener varias aplicaciones más. Un túnel es básicamente un método para encapsular un protocolo en otro. La existencia de protocolos no enrutables hacen que el uso de las VPN sea imprescindible para enviar el tráfico que utiliza este tipo de protocolos. Incluso para otros tipos de protocolos enrutables cuya dificultad de enrutamiento es elevada, se hace más sencillo cuando este se envía por un túnel.

Otra buena razón para la utilización de túneles es evitar los problemas que suelen dar los protocolos de enrutamiento en redes extremadamente grandes debido a que muchas veces su arquitectura no coincide en tipos de protocolos o entre áreas.

Los túneles son sumamente útiles en laboratorios o ambientes de prueba donde se intenta emular las topologías de red más complejas.

Existen muchas variaciones diferentes para la configuración de las VPN, aun para las más comunes. En el caso de este libro se utilizará como ejemplo de configuración la de túneles **GRE** (*Generic Routing Encapsulation*) que es una norma abierta. Existen varias versiones de GRE, la versión 0 es la común, la versión 1 también llamada **PPTP** (*Point to Point Tunneling Protocol*) incluye una capa intermedia PPP, mientras que GRE soporta directamente protocolos de capa 3 como IP e IPX. GRE no utiliza TCP ni UDP, trabaja directamente con IP, identificado con el número 47. Posee características propias de entrega, verificación e integridad.

10.8.1 Funcionamiento de las VPN

- Los routers encapsulan los paquetes IP con la etiqueta **GRE** y los envían por la red al router de destino al final del túnel, el router remoto desencapsula los paquetes quitándoles la etiqueta GRE dejándolos listos para enrutarlos localmente. El paquete GRE pudo haber cruzado una gran cantidad de router para alcanzar su destino, sin embargo para este, solo ha efectuado un único salto hacia el destino. Esto significa que en el encabezado IP el tiempo de vida del paquete TTL (*Time To Live*) se ha incrementado una vez.

Existen otros protocolos como **IP-in-IP** (IP sobre IP) que utiliza el número 4 de referencia de protocolo. Es un protocolo abierto pero aun así GRE ofrece mayor flexibilidad particularmente con los routers Cisco.

La utilización de las VPN obliga muchas veces a los routers a segmentar los paquetes para enviarlos a través del túnel debido a que su tamaño excede la MTU (Unidad de Transmisión Máxima) que estos pueden soportar. En ciertos casos pueden existir dificultades con las aplicaciones que ven las cabeceras de los paquetes IP duplicadas, sin embargo, esto ocurre en raros casos. Cuando el router no puede segmentar el paquete debe descartarlos, en estos casos envía mensajes ICMP al dispositivo origen para que regule el tamaño de los paquetes. Como resultado final de este proceso es que para el uso eficaz de las VPN el tamaño de las MTU debe reducirse.

Básicamente las VPN deben proporcionar:

- Confidencialidad.
- Integridad.
- Autenticación.

10.8.2 IPSec

IPSec (Protocolo de Internet Seguro) es un conjunto de protocolos y algoritmos de seguridad diseñados para la protección del tráfico de red para trabajar con IPv4 e IPv6 de modo transparente o modo túnel que soporta una gran variedad de encriptaciones y autenticaciones. El principio básico de funcionamiento de IPSec es la independencia algorítmica que le permite efectuar cambios de algoritmos si alguien descubre un fallo crítico o si existe otro más eficaz.

IPSec está diseñado para proporcionar seguridad sobre la capa de red IP, por lo tanto, puede ser utilizado eficazmente sobre protocolos como TCP, UDP, ICMP y otros. Esto es muy importante porque significa que se puede usar IPSec con protocolos o aplicaciones inseguras logrando un excelente nivel de seguridad global.

IPSec se introdujo para proporcionar servicios de seguridad tales como:

- Encriptar el tráfico de manera segura para que no pueda ser leído por nadie más que las partes a las que está dirigido.
- Validar la integridad de los datos, asegurando que el tráfico no ha sido modificado a lo largo de su trayecto.

- Autenticar a los extremos reconociendo el tráfico que proviene de un extremo seguro y validado.

- Anti-repetición evitando la repetición de la sesión segura.

Lamentablemente, debido a la gran proliferación de protocolos y algoritmos, algunos propietarios, como **ISAKMP** (*Internet Security Association Key Management Protocol*), **IKE** (*Internet Key Exchange*) o **DH** (*Diffie-Hellman*), pueden producir confusiones a la hora de las configuraciones. Particularmente desarrollaremos los casos más comunes.

IPSec utiliza dos protocolos importantes de seguridad:

- **AH** (*Authentication Header*) incluye un sistema de autenticación criptográfico en el encabezado del paquete IP que le permite asegurar que los datos no se han manipulado de forma alguna, y que realmente viene del dispositivo de la fuente correcta. AH no encripta directamente los datos.

- **ESP** (*Encapsulating Security Payload*) proporciona encriptación a la carga útil del paquete para el envío seguro de los datos. Se utiliza para proteger tanto la conexión como los datos. La mayor parte de sistemas utilizan ESP.

La autenticación y la encriptación se utilizan en funciones completamente diferentes pero absolutamente complementarias. Al usar IPSec, es sumamente recomendable el uso de ambos protocolos.

10.8.3 Modos de operación de IPSec

IPSec tiene dos modos principales de funcionamiento, modo **túnel** y modo **transporte**. En el modo túnel, todo el paquete IP (datos más cabeceras del mensaje) es cifrado y/o autenticado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento. El modo túnel se utiliza para comunicaciones red a red, VPN. En modo transporte, solo la carga útil (los datos que se transfieren) del paquete IP es cifrada y/o autenticada. El enrutamiento permanece intacto, ya que no se modifica ni se cifra la cabecera IP. Este método se usa para comunicaciones de ordenador a ordenador.

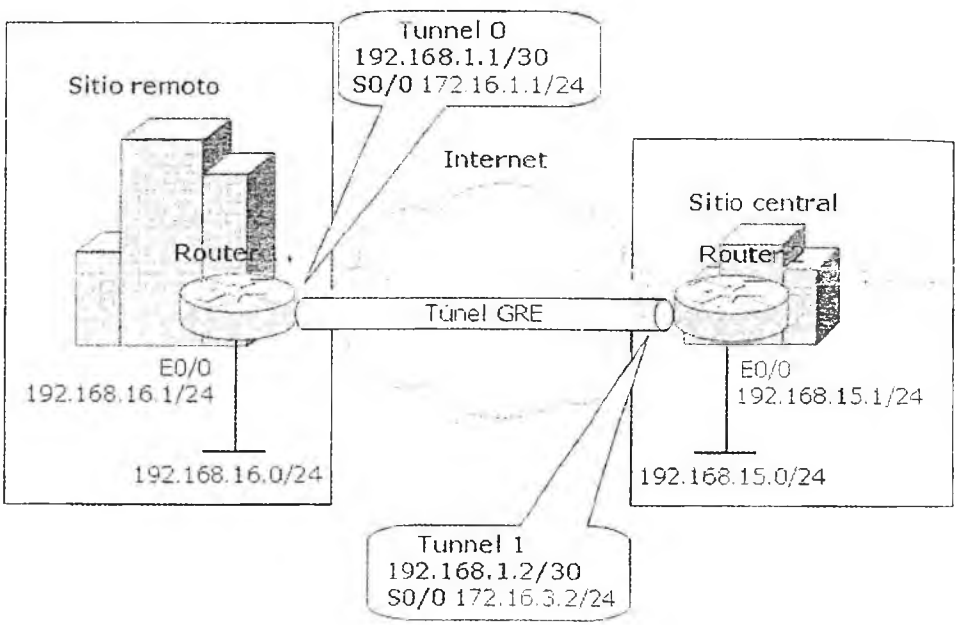
Cuando se utiliza la cabecera de autenticación (AH), las direcciones IP no pueden ser traducidas, debido al cifrado que sufren los datos. Las capas de transporte y aplicación están siempre aseguradas por un encriptado, de forma que

no pueden ser modificadas de ninguna manera (por ejemplo, traduciendo los números de puerto TCP y UDP). Una forma de encapsular mensajes IPSec para atravesar NAT es utilizando **NAT-T** (*NAT Traversal*).

10.9 CASO PRÁCTICO

10.9.1 Configuración de una VPN de router a router

Se describe a continuación la configuración de un túnel GRE en una VPN de router a router según la siguiente topología.



Router 1:

```
Router1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#crypto isakmp policy 10
Router1(config-isakmp)#encr aes 256
Router1(config-isakmp)#authentication pre-share
Router1(config-isakmp)#group 2
```

```
Router1(config-isakmp)#exit
Router1(config)#crypto isakmp key TUNEL01 address 172.16.2.1 no-
xauth
Router1(config)#crypto ipsec transform-set TUNNEL TRANSFORM ah-sha-
hmac esp-aes 256
Router1(cfg-crypto-trans)#mode transport
Router1(cfg-crypto-trans)#exit
Router1(config)#crypto map TUNELMAPA 10 ipsec-isakmp
Router1(config-crypto-map)#set peer 172.16.2.1
Router1(config-crypto-map)#set transform-set TUNNEL-TRANSFORM
Router1(config-crypto-map)#match address 102
Router1(config-crypto-map)#exit
Router1(config)#access-list 102 permit gre host 172.16.1.1 host
172.16.2.1
Router1(config)#interface Tunnel0
Router1(config-if)#ip address 192.168.1.1 255.255.255.252
Router1(config-if)#tunnel source 172.16.1.1
Router1(config-if)#tunnel destination 172.16.2.1
Router1(config-if)#exit
Router1(config)#interface Serial 0/0
Router1(config-if)#ip address 172.16.1.1 255.255.255.0
Router1(config-if)#ip access-group 101 in
Router1(config-if)#crypto map TUNELMAPA
Router1(config-if)#exit
Router1(config)#interface FastEthernet0/0
Router1(config-if)#ip address 192.168.16.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#access-list 101 permit gre host 172.16.2.1 host
172.16.1.1
Router1(config)#access-list 101 permit esp host 172.16.2.1 host
172.16.1.1
Router1(config)#access-list 101 permit udp host 172.16.2.1 host
172.16.1.1 eq isakmp
Router1(config)#access-list 101 permit ahp host 172.16.2.1 host
172.16.1.1
Router1(config)#access-list 101 deny ip any any log
Router1(config)#interface Loopback0
Router1(config-if)#ip address 192.168.16.1 255.255.255.0
Router1(config-if)#exit
Router1(config)#ip route 192.168.15.0 255.255.255.0 Tunnel 0
Router1(config)#end
```

Router 2:

```
Router2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#crypto isakmp policy 10
Router2(config-isakmp)#encr aes 256
Router2(config-isakmp)#authentication pre-share
Router2(config-isakmp)#group 2
```

```
Router2(config-isakmp)#exit
Router2(config)#crypto isakmp key TUNEL01 address 172.16.1.1
Router2(config)#crypto ipsec transform-set TUNNEL-TRANSFORM ah-sha-
hmac esp-aes 256
Router2(cfg-crypto-trans)#mode transport
Router2(cfg-crypto-trans)#exit
Router2(config)#crypto map TUNELMAPA 10 ipsec-isakmp
Router2(config-crypto-map)#set peer 172.16.1.1
Router2(config-crypto-map)#set transform-set TUNNEL-TRANSFORM
Router2(config-crypto-map)#match address 102
Router2(config-crypto-map)#exit
Router2(config)#access-list 102 permit gre host 172.16.2.1 host
172.16.1.1
Router2(config)#interface Tunnel1
Router2(config-if)#ip address 192.168.1.2 255.255.255.252
Router2(config-if)#tunnel source 172.16.2.1
Router2(config-if)#tunnel destination 172.16.1.1
Router2(config-if)#exit
Router2(config)#interface Serial 0/0
Router2(config-if)#ip address 172.16.2.1 255.255.255.0
Router2(config-if)#ip access-group 101 in
Router2(config-if)#crypto map TUNELMAPA
Router2(config-if)#exit
Router2(config)#interface FastEthernet0/0
Router2(config-if)#ip address 192.168.15.1 255.255.255.0
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config)#access-list 101 permit gre host 172.16.1.1 host
172.16.2.1
Router2(config)#access-list 101 permit esp host 172.16.1.1 host
172.16.2.1
Router2(config)#access-list 101 permit udp host 172.16.1.1 host
172.16.2.1 eq isakmp
Router2(config)#access-list 101 permit ahp host 172.16.1.1 host
172.16.2.1
Router2(config)#access-list 101 deny ip any any log
Router2(config)#interface Loopback0
Router2(config-if)#ip address 192.168.15.1 255.255.255.0
Router2(config-if)#exit
Router2(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2
Router2(config)#ip route 192.168.16.0 255.255.255.0 Tunnel 1
Router2(config)#end
```

10.10 ACCESO REMOTO

10.10.1 Acceso por cable

Las tecnologías de acceso por cable son actualmente las más populares y proporcionan conectividad mediante redes MAN a comunidades, edificios, empresas, etc. Es posible efectuar transmisiones de señales de televisión, conexión a Internet y telefonía por el mismo medio.

La transmisión múltiple de señales a través de un cable se realiza por medio de la modulación de la señal. La modulación es la adición de información a una señal portadora electrónica u óptica. La voz utiliza solamente una pequeña parte de la frecuencias disponibles en los cables de par trenzado.

10.10.2 Acceso por DCL

Las líneas DSL (*Digital Suscriber Line*) son soluciones comunes de acceso que cuentan con la ventaja añadida de que se pueden utilizar sobre la infraestructura telefónica existente, lo que hace innecesario desplegar un nuevo cable para su implementación.

La implementación de esta tecnología es económica gracias al uso del cableado existente pero guarda ciertas limitaciones como:

- La distancia del proveedor al cliente.
- Interferencias de radiofrecuencia.
- No puede ser implementada sobre fibra óptica.
- Atenuación y degradación de la señal en largas distancias.

Existen dos variantes de DSL:

- ADSL, DSL Asimétrica. Las velocidades de subida y bajada son diferentes. Es la más popular para uso domestico o pequeñas oficinas.
- SDSL, ASL Simétrica. Las velocidades de subida y bajada son idénticas.

10.11 FUNDAMENTOS PARA EL EXAMEN

- Estudie las terminologías, estándares y conexiones utilizadas en las redes WAN.
- Recuerde los tipos de encapsulación de capa 2 de las redes WAN.
- Memorice los conceptos sobre PPP y los pasos en el establecimiento de una sesión PPP.
- Tenga en cuenta los tipos de autenticaciones PPP y sus diferencias fundamentales.
- Estudie los fundamentos sobre NAT, los diferentes tipos de configuraciones y para qué se utilizan en cada caso.
- Recuerde las terminologías empleadas en la tarea de configuración de NAT.
- Analice el proceso de traslación de una dirección IP a otra.
- Recuerde los fundamentos de Frame-Relay, sus terminologías y funcionamiento.
- Analice el funcionamiento de las diferentes topologías Frame-Relay y qué tipo de subinterfaz se utiliza en cada caso.
- Recuerde exactamente los tipos de encapsulado, LMI y DLCI que utiliza Frame-Relay.
- Estudie los fundamentos y funciones de una VPN.
- Analice la seguridad que debe proporcionar una VPN y el funcionamiento de IPSec.
- Estudie, analice y ejercite en dispositivos reales o en simuladores todos los comandos necesarios para las configuraciones de PPP, NAT y Frame-Relay y todos los comandos para su verificación.
- Recuerde las tecnologías de acceso remoto, analice para qué emplearía cada una.

Apéndice A

PREPARATIVOS PARA EL EXAMEN

11.1 VISIÓN GENERAL DEL EXAMEN

A partir de 1998, Cisco Systems, Inc. anunció una nueva iniciativa de desarrollo profesional llamada *Cisco Career Certifications*. Hasta la fecha estas certificaciones han satisfecho las exigencias de los mejores profesionales y empresas del mercado.

La certificación **CCNA** (*Cisco Certified Network Associate*) es una de las certificaciones a nivel mundial más popular y valorada por las industrias informáticas y la base fundamental para entrar al mundo de las comunicaciones de datos. Estar en poder de esta certificación abre las puertas a todos aquellos que pretenden avanzar hacia certificaciones profesionales tales como el CCNP, CCDP o CCSP. Un técnico CCNA está capacitado para realizar tareas tales como:

- Instalar y configurar routers y switches Cisco y otros.
- Llevar a cabo tareas de mantenimiento en redes multiprotocolo LAN y WAN.
- Desarrollar tareas de soporte de Nivel 1.
- Mejorar y asegurar el rendimiento de las redes.

Los conocimientos de un técnico CCNA incluyen entre otros:

- Manejar y configurar protocolos de enrutamiento.
- Conocer y configurar tecnologías de acceso.
- Administrar y configurar seguridad a través de listas de acceso.
- Crear y dar soporte a redes virtuales, etc.

Un técnico certificado puede desarrollar un abanico de tareas profesionales que van desde tareas de campo hasta soporte técnico incluyendo tareas de pre o post venta e instalaciones.

11.1.1 Titulación y certificación

La exigencia laboral en la actualidad ha llevado a que los postulantes a diferentes puestos de trabajo posean una severa preparación, no solo a nivel universitario y lingüístico sino también en especializaciones de diversos fabricantes. Estas especializaciones convalidan conocimientos, habilidades y requisitos propios de ese fabricante, que es lo que se llama certificación.

Una certificación es, entonces, una calificación obtenida por una persona a través de un organismo certificador que ha cumplido con los requisitos mínimos impuestos por dicha corporación. Las empresas o fabricantes utilizan estos organismos como herramientas para otorgar sus certificaciones a través de evaluaciones teórico prácticas, no obstante estos no intervienen en la elaboración de los tópicos o temarios que son propios de cada fabricante.

En este caso el valor añadido de la certificación CCNA es su valía en el mercado laboral.

Una persona en posesión de un título de grado académico puede completar su capacitación a través de una o varias certificaciones acorde a las tareas que desee desarrollar en su ámbito laboral. Por lo tanto, una certificación como el CCNA permite, por ejemplo, que un Ingeniero en Telecomunicaciones que posee un abanico muy amplio de conocimientos pueda especializarse aun más, o que un Ingeniero Industrial pueda re-orientar su formación hacia otros aspectos de la vida laboral. Lo que es aún igual de importante es la posibilidad que brinda la certificación a todos aquellos que por diversas circunstancias no poseen títulos académicos y quieran especializarse.

11.1.2 Requisitos para el examen

Como se dijo en los párrafos anteriores, la obtención de una certificación se consigue a través de un organismo certificador, como puede serlo, en el caso del CCNA, la empresa VUE (http://www.vue.com).

Los requisitos de edad para presentarse al examen de certificación CCNA deben cumplir las políticas de privacidad de Cisco y son los siguientes:

- Los menores de 13 años no pueden presentarse al examen.
- Las personas de entre 13 y 17 años pueden presentarse al examen de certificación con el consentimiento de los padres o tutores.
- Las personas mayores de 18 años pueden presentase sin ningún tipo de restricción.

No es necesario poseer ninguna titulación académica o certificación previa. Sin embargo, el CCNA será un requisito previo para otras certificaciones profesionales.

Los candidatos deben asumir el compromiso de integridad y confidencialidad de Cisco prohibiendo acciones que describan cualquier información acerca del examen de certificación.

(http://www.cisco.com/web/learning/downloads/Cisco-Career-Certifications-and-Confidentiality-Agreement_v13.pdf)

11.1.3 Características del examen

Actualmente existen dos formas de obtener la certificación CCNA, a través de uno o dos exámenes. Siendo la mejor recomendación hacerlo por la vía rápida, es decir un solo examen. Los tipos y números de exámenes son los siguientes:

- En un solo examen: **640-802 CCNA**.
- En dos exámenes:
  - **640-822 ICND 1**
  - **640-816 ICND 2**

Las características del examen son las siguientes:

- Duración: 90 minutos. El examen en inglés en países hispano parlantes, se suman 20 minutos más.
- Cantidad de preguntas: aproximadamente 55. Mínimo dos simuladores de routers. Existe una base de datos de donde se seleccionan aleatoriamente las preguntas.
- Idiomas: inglés, español, chino, ruso, coreano, francés, portugués y japonés.
- Aprobación: 849 sobre 1000. El puntaje asignado a cada pregunta puede variar, incluso cabe la posibilidad de que algunas preguntas no puntúen.
- Fechas y horarios: según la disponibilidad de los centros de examinación.

Personalmente recomiendo el examen 802 en el idioma local, quien diga que le ha ido mal en el examen porque la traducción es errónea es porque no ha estudiado lo suficiente.

El examen consta de diferentes tipos y modalidades de preguntas:

- Respuesta única a partir de opciones múltiples.
- Respuestas múltiples a partir de opciones múltiples.
- Respuestas tipo "drag and drop".
- Completar los espacios en blanco.
- Configuración de routers con simulador.

Los contenidos del examen CCNA 640-802 pueden resumirse en:

- Principios de networking.
- Modelo OSI y TCP/IP.
- Implementación de subredes y VLSM.
- Administración del Cisco IOS.
- Enrutamiento IP.
- Administración de redes Cisco.
- Conmutación LAN, VLAN y trunking.
- Redes wireless LAN.
- Listas de control de acceso.
- Tecnologías WAN.

Para más información sobre localización de centros de certificación autorizados, requisitos, horarios, precios u otro tipo de información puede consultarse la Web de Pearson-Vue en *http://www.vue.com*.

http://www.cisco.com/web/learning/downloads/Cisco-Career-Certifications-and-Confidentiality-Agreement_v13.pdf.

Para mayor información respecto a duración de los exámenes, idiomas disponibles o cualquier otro tipo de duda sobre la certificación CCNA es posible consultar la Web de Cisco en:

http://www.cisco.com/web/learning/le3/le2/le37/le10/learning_certification_type_home.html.

Es importante resaltar que una vez iniciado el examen no se puede retroceder en la secuencia de las preguntas, ni que se puede avanzar dejando la respuesta en blanco, es decir, sin responder.

Las certificaciones suelen tener un tiempo de caducidad, en el caso del CCNA el tiempo de validez de la certificación es de tres años. Puede re-certificarse con un examen similar, o antes de la fecha de caducidad con cualquier examen superior tipo **642-XXX**.

11.1.4 Preparativos para el examen

Aprobar el examen de certificación no es una tarea fácil pero tampoco imposible. Existen diferentes maneras de preparación, que van desde cursos bajo la plataforma de Cisco (CNAP), cursos intensivos (ICND) o libre a través de diferentes bibliografías y prácticas. Lo único y fundamental aunque parezca una obviedad, es estudiar.

En lo personal y después de varios años de experiencia docente y recabando información de los propios alumnos debo decir que ningún método es perfecto y que hacer recomendaciones es una tarea delicada. Si se es alumno de una academia una vez finalizado el curso completo se debe centrar la atención en el examen, no es lo mismo prepararse para el examen de certificación que para un curso. Si la intención es presentarse por cuenta propia se deben estudiar a fondo todos los conceptos contenidos en el examen incluso los más insignificantes, no sirve de nada la experiencia laboral, son ideas diferentes. Como ejemplo, son típicos los casos de alumnos avanzados, con amplia experiencia laboral con routers y switches pero que no sabían crear subredes (una de las cuestiones mínimas indispensables de las que hablaba), el fracaso es rotundo.

11.1.5 Recomendaciones para la presentación al examen

No hay truco ni magia. Realizar test de preguntas, estudiar en grupo, consultar toda la bibliografía disponible, Internet es lo más obvio. Muchas veces un aluvión de nuevos conocimientos puede ser contraproducente. Cuando un alumno desaprueba reiteradas veces, seguramente no será porque le falten conocimientos, sino porque le falte exactitud, rapidez y confianza.

Previo a comenzar el examen se podrán hacer las anotaciones necesarias como ayuda memoria. Controlar el tiempo cada cierto periodo. Si estando en la pregunta 30, por ejemplo quedan 20 minutos es un mal pronóstico.

Tener siempre en cuenta que no es posible volver atrás, y que no se puede avanzar sin responder. Probar el correcto funcionamiento de las topologías de los simuladores y guardar las configuraciones con el comando respectivo. Los comandos ayuda no funcionan, estudiar los comandos completos.

Las preguntas que siguen a continuación son una base de ayuda para el examen, de ninguna manera son garantía de aprobación sin el conocimiento adecuado. Se han realizado cuidadosamente intentando que se parezcan lo más posible al examen.

11.2 CUESTIONARIO TEMATICO

1. ¿Qué tipo de conmutación LAN espera a que la ventana de colisión pase antes de mirar la dirección de hardware de destino en la tabla de filtro MAC y enviar la trama?

   A. Método de corte.
   B. Almacenamiento y envío.
   C. Verificación de fragmentos.
   D. Libre de fragmentos.

   Respuesta: D
   Página: 219

2. ¿Cuál de los comandos que se proponen a continuación deberá seguir a esta línea de comandos?

```
access-list 110 deny tcp any any eq ftp
```

   A. `access-list 110 deny ip any any`
   B. `access-list 110 deny tcp any any`

C. `access-list 110 permit ip any`
D. `access-list 110 permit ip any any`

Respuesta: D
Página: 207

3. ¿Cuántos tipos de LMI están disponibles en los routers Cisco?

A. Dos.
B. Tres.
C. Cuatro.
D. Cinco.

Respuesta: B
Página: 270

4. Considerando una máscara de subred 255.255.255.224, ¿cuál de las siguientes direcciones puede ser asignada a un nodo de red? (elija 3)

A. 15.234.118.63
B. 92.11.178.93
C. 134.178.18.56
D. 192.168.16.87
E. 201.45.116.159
F. 217.63.12.192

Respuesta: B, C, D
Página: 71

5. Se ha asignado a su cargo a un técnico novato que necesita saber cuál de los siguientes modos son válidos cuando un puerto del switch se utiliza como un troncal de VLAN. ¿Qué podría decirle? (elija 3 opciones).

A. Bloquing.
B. Auto.
C. Desirable.
D. On.
E. Transparent.
F. Learning.

Respuesta: B, C, D
Página:243

6. ¿Cuáles son los tres comandos que se pueden utilizar para verificar listas de acceso IP?

   A. show interfaces
   B. show ip interfaces
   C. show running-config
   D. show access-lists

Respuesta: B, C, D
Página: 213

7. Se ha adquirido un router que estaba operativo en otra empresa, y lo ha configurado en su laboratorio de acuerdo a las necesidades de su red. Luego de completar las tareas de configuración ha ejecutado el comando **copy runningconfig startup-config** para guardar su configuración en la NVRAM. Acaba de apagar el dispositivo y lo ha instalado en el rack de producción. Después de conectar nuevamente el router, ha encendido el dispositivo y este arrancó en modo **setup**. Ha entrado en el modo privilegiado y al ejecutar un **show startup-config** puede comprobar que su configuración se encuentra allí.

   ¿Cuál de las siguientes podría ser la causa del problema?

   A. Un fallo en el hardware del router que determina que este no lea la configuración almacenada en la NVRAM.
   B. La configuración de respaldo guardada en la flash se ha corrompido y no puede ser analizada.
   C. El registro de configuración está configurado para saltear la lectura del archivo de configuración.
   D. La configuración de respaldo en la NVRAM se ha corrompido y no puede ser analizada.

Respuesta: D
Página: 109

8. ¿Cuál de las siguientes es una métrica por defecto utilizada por RIP? (elija 2).

   A. 16 ms.
   B. Cantidad de routers en la red.
   C. Número de saltos.
   D. 16 saltos = inalcanzable.
   E. Último salto disponible.

Respuesta: C, D
Página: 150

9. ¿Cuál de las siguientes listas de acceso permitirá solo tráfico HTTP a la red 196.15.7.0?

   A. `access-list 100 permit tcp any 196.15.7.0 0.0.0.255 eq www`
   B. `access-list 10 deny tcp any 196.15.7.0 eq www`
   C. `access-list 100 permit 196.15.7.0 0.0.0.255 eq www`
   D. `access-list 110 permit ip any 196.15.7.0 0.0.0.255`
   E. `access-list 110 permit www 196.15.7.0 0.0.0.255`

Respuesta: A
Página: 202

10. ¿Cuál de las siguientes afirmaciones es verdadera respecto de la secuencia de comandos que se muestra más abajo? (elija todas las que se apliquen).

```
Router(config)#interface loopback 0
Router(config-if)#ip address 192.168.16.24 255.255.255.255
```

   A. Crea una interfaz virtual, solo a nivel de software.
   B. Provee una vía para verificar la convergencia de las actualizaciones de enrutamiento OSPF.
   C. La mascara de subred 255.255.255.255 se denomina máscara de nodo.
   D. Utiliza una máscara de wildcard de 255.255.255.255
   E. Asegura que la interfaz está siempre activa para los procesos OSPF.
   F. Este comando puede ser utilizado exclusivamente para configurar interfaces seriales.

Respuesta: A, C
Página: 120, 73

11. Se ha dispuesto realizar una actualización de la documentación de la red. Una de las tareas que se consideran es la documentación del nombre de la imagen del IOS de cada router de la red. ¿Qué comando deberá utilizar para encontrar esta información?

   A. `Router#show protocols`
   B. `Router#show version`
   C. `Router#show imagen`
   D. `Router#show IOS`

E. `Router#show flash`

Respuesta: B
Página: 121

12. ¿Cuál de los siguientes comandos mostrará la lista de acceso extendida 187? (elija 2).

A. `show ip interfaces`
B. `show ip access-lists`
C. `show access-lists 187`
D. `show access-lists 187 extended`

Respuesta: B, C
Página: 213

13. ¿Cuál de las siguientes opciones es proporcionada por el comando **show cdp entry *?** (elija todas las que se apliquen).

A. Dirección IP del router colindante.
B. Información del protocolo.
C. Plataforma.
D. Capacidad.
E. Tiempo.
F. ID del puerto.
G. Tiempo de espera.
H. La misma información que show version.
I. La ID del dispositivo colindante.
J. La interfaz local.
K. La velocidad del enlace.

Respuesta: A, B, C, D, F, G, I, J
Página: 136

14. ¿Para qué se utiliza la distancia administrativa en el enrutamiento?

A. Determinar al administrador de red para entrar en esa ruta.
B. Crear una base de datos.
C. Calificar la confiabilidad del origen, expresada como un valor numérico de 0 a 255.
D. Calificar la confiabilidad del origen, expresada como un valor numérico de 0 a 1023.

Respuesta: C
Página: 91, 92

15. ¿Cuáles de los siguientes protocolos incluye la suite PPP? (elija 3).

A. HDLC
B. LCP
C. SDLC
D. NCP
E. LAPB

Respuesta: A, B, D
Página: 257

16. ¿Cómo se denominan las unidades de datos de protocolo en la capa de enlace de datos?

A. Tramas.
B. Paquetes.
C. Datagramas.
D. Transportes.
E. Segmentos.
F. Bits.

Respuesta: A
Página: 48, 49

17. ¿Cuál es el protocolo y cuál es el propósito de la siguiente dirección?

238.255.255.255

A. IPX, un broadcast SAP.
B. IP, una dirección de multicast.
C. IP, una dirección reservada.
D. IP, una dirección de broadcast.
E. IPX, un broadcast inundado.
F. IP, una dirección de unicast.

Respuesta: B
Página: 68

18. ¿Cuáles son los cuatro estados que atraviesa un puerto de un switch que implementa el Protocolo de Árbol de Expansión (STP)?

A. Aprendiendo.
B. Aprendido.
C. Escuchado.
D. Oído.
E. Escuchando.
F. Enviando.
G. Enviado.
H. Bloqueando.
I. Reuniendo.

Respuesta: A, E, F, H
Página: 224

19. ¿Cuál de los siguientes elementos es utilizado por las listas de acceso IP extendidas como base para permitir o denegar paquetes?

A. Dirección de origen.
B. Dirección de destino.
C. Protocolo.
D. Puerto.
E. Todas las anteriores.

Respuesta: E
Página: 196

20. ¿Qué protocolo se utiliza con PPP para establecer, configurar y autenticar una conexión de enlace de datos?

A. LCP.
B. NCP.
C. HDLC.
D. X.25.

Respuesta: A
Página: 257

21. Si estuviera diseñando una red y necesitara dividir los dominios de colisión, ¿en qué capa del modelo Cisco proporcionaría esta función?

A. Física.
B. De acceso.
C. Principal.
D. De red.
E. De distribución.

F. De enlace de datos.

Respuesta: B
Página: 52

22. Frame-Relay implementa un recurso que le permite prevenir la caída del PVC por falta de actividad. ¿Cuál es el nombre de este recurso?

A. DLCI.
B. BECN.
C. FECN.
D. LMI.
E. CIR.
F. De.

Respuesta: D
Página: 269

23. ¿Qué es horizonte dividido?

A. Cuando un router reconoce a qué interfaz ha llegado una actualización y no publica esa información a través de la misma interfaz.
B. Cuando se tiene una red física de bus grande y este divide el tráfico.
C. Impide que las actualizaciones regulares hagan difusión a través de un enlace inactivo.
D. Evita que los mensajes de actualización regulares vuelvan a anunciar que una ruta está inactiva.

Respuesta: A
Página: 96

24. ¿Cuáles de los siguientes son dos tipos de PDU que pertenecen a la capa de red?

A. Datos.
B. Rutas.
C. Estáticos.
D. Dinámicos.
E. Principal.
F. Segmentos.

Respuesta: A, B
Página: 48, 49

25. ¿Cuáles de los siguientes son protocolos de la capa de aplicación que forman parte de la suite TCP/IP? (elija 3).

    A. ARP.
    B. HTTP.
    C. SMTP.
    D. FTP.
    E. ICMP.

Respuesta: B, C, D
Página: 55

26. ¿Cuál es el comando correcto para configurar como identificación del router el nombre **Spain**, que un administrador vería al conectarse por Telnet o a través de la consola?

    A. `description Spain Router`
    B. `banner motd $ Spain $`
    C. `hostname Spain`
    D. `host name Spain`
    E. `set prompt Spain`

Respuesta: C
Página: 112

27. Al iniciar un router por primera vez, ¿desde dónde se carga por defecto el Cisco IOS?

    A. Boot ROM.
    B. NVRAM.
    C. Flash.
    D. ROM.

Respuesta: C
Página: 104, 108

28. Haga coincidir los números decimales y hexadecimales de la izquierda con sus correspondientes expresiones en formato binario en la columna de la derecha. No todas las opciones de la izquierda tienen correspondencia en la derecha.

0xf1
0x1f
192
96
0x9f
0xf9
85
170

10101010
11000000
11110001
11110001

Respuesta:

10101010 es 170 en notación decimal,
11000000 es 192 en notación decimal,
11110001 es f1 en notación hexadecimal o 241 en decimal,
10011111 es 9f en notación hexadecimal o 159 en decimal.

Página: 63

29. ¿Para qué se utiliza IARP?

A. Mapear direcciones X.21 a direcciones X.25.
B. Mapear DLCI a direcciones de protocolo de red.
C. Direccionamiento SMDS.
D. Mapear direcciones ATM a direcciones virtuales.

Respuesta: B
Página: 269, 270

30. ¿Qué dirección de difusión utilizará el host 192.168.210.5 255.255.255.252?

A. 192.168.210.255
B. 192.168.210.254
C. 192.168.210.7
D. 192.168.210.15

Respuesta: C
Página: 71

31. ¿En qué capa del modelo OSI se convierte la información codificada en 1s y 0s en una señal digital?

A. Física.
B. Transporte.

C. Enlace de datos.
D. Red.

Respuesta: A
Página: 23, 24

32. Si necesita tener una dirección de red Clase B dividida en 510 subredes, ¿qué máscara de subred debe asignar?

A. 255.255.255.252
B. 255.255.255.128
C. 255.255.0.0
D. 255.255.255.192

Respuesta: B
Página: 71

33. ¿Para qué necesita un DLCI de Frame-Relay el Router_A al momento de encapsular una trama?

A. Definir la señalización estándar entre el Router_A y el switch.
B. Identificar el circuito entre el Router_A y el switch.
C. Identificar el circuito entre el Router_B y el switch.
D. Identificar la encapsulación utilizada entre Router_A y Router_B.
E. Definir la señalización estándar entre Router_B y el switch.

Respuesta: C
Página: 268, 270

34. Existe una línea dedicada configurada en una pequeña oficina que se conecta con las oficinas corporativas. La compañía desea tener una línea de respaldo económica en caso de que la línea dedicada salga de servicio.

¿Qué tipo de servicio WAN elegiría para respaldar la línea dedicada?

A. Frame-Relay con SVC.
B. Línea dedicada.
C. ADSL.
D. ATM.

Respuesta: C
Página: 285

35. ¿En qué capa del modelo Cisco se definirían los dominios de difusión?

A. Principal.
B. De red.
C. Física.
D. Distribución.
E. Acceso.
F. Transporte.

Respuesta: D
Página: 52

36. Dos switches, llamados Madrid y Córdoba, han sido configurados para utilizar VTP, pero no están compartiendo los mensajes VTP. De acuerdo a la información que se muestra en las siguientes sintaxis, ¿a qué se debe?

```
Madrid#show vtp status
VTP versión: 2
Configuration Revision: 0
Maximum VLANs supported locally: 64
Number of existing VLANs: 5
VTP Operating Mode: Server
VTP Domain Name: Salta
VTP Prunning Mode: Disabled
VTP V2 Mode: Disabled
VTP Traps Generation Disabled
```

```
Cordoba#show vtp status
VTP versión: 2
Configuration Revision: 0
Maximum VLANs supported locally: 64
Number of existing VLANs: 5
VTP Operating Mode: Server
VTP Domain Name: Cordoba
VTP Prunning Mode: Disabled
VTP V2 Mode: Disabled
VTP Traps Generation Disabled
```

A. El modo VTP V2 no está en operación.
B. El modo de recorte VTP está deshabilitado.
C. El nombre de dominio VTP está configurado incorrectamente.
D. No se ha configurado para que opere en modo VTP.
E. La versión de VTP está mal configurada.

Respuesta: C
Página: 229, 248

37. ¿Cuáles son los dos comandos que muestran la tabla de direcciones MAC?

A. `show mac address-table`
B. `show mac-address-table`
C. `show table mac address`
D. `show ip route mac table`

Respuesta: A, B
Página: 238

38. ¿Cuál de los siguientes comandos globales configurará de modo estático el número máximo de direcciones MAC que pueden ser asignadas a una interfaz del switch?

A. `interface vlan 1 maximum [value]`
B. `interface vlan1-maximum [value]`
C. `shitch port security maximaum [value]`
D. `shitchport port-security maximaum [value]`
E. `shitchport port security maximaum [value]`

Respuesta: D
Página: 238

39. ¿Qué comando se utiliza para impedir que las actualizaciones de enrutamiento se publiquen a través de una interfaz en particular?

A. `Router(config-if)#no router rip`
B. `Router(config-if)#passive-interface`
C. `Router(config-router)#passive-interface s0`
D. `Router(config-if)#passive-interface s0`
E. `Router(config-router)#no routing updates`

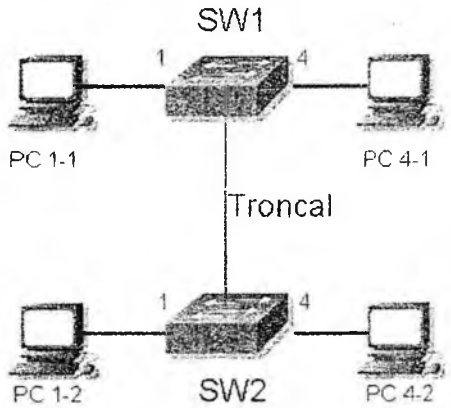
Respuesta: C
Página: 152

40. ¿En qué capa del modelo OSI se deben ubicar los puentes?

A. Física.
B. Transporte.
C. Enlace de datos.
D. Red.

Respuesta: C
Página: 31

41. Tomando en consideración el diagrama de red que se presenta, asuma que los puertos 1 a 3 están asignados a la VLAN1 y los puertos 4 a 6 están asignados a la VLAN 2 en cada switch. Los switches están interconectados a través de un enlace troncal. ¿Cuál de las siguientes condiciones verificará la propiedad de las VLAN y la operación del troncal? (elija 3).



A. El nodo 1-1 puede hacer ping al nodo 1-2.
B. El nodo 1-1 puede hacer ping al nodo 4-2.
C. El nodo 1-1 no puede hacer ping al nodo 1-2.
D. El nodo 4-1 no puede hacer ping al nodo 1-2.
E. El nodo 4-1 puede hacer ping al nodo 4-2.

Respuesta: A, D, E
Página: 225

42. Su gerente está interesado en las diferencias entre los sistemas Ethernet half-duplex y full-duplex. ¿Cuáles de las siguientes afirmaciones son verdaderas respecto de Ethernet half-duplex? (elija 2).

A. Ethernet half-duplex opera en dominios de colisión compartidos.
B. Ethernet half-duplex opera en dominios de colisión privados.
C. Ethernet half- duplex tiene un ancho de banda efectivo mayor.
D. Ethernet half-duplex tiene un ancho de banda efectivo menor.
E. Ethernet half-duplex opera en un dominio de difusión privado.

Respuesta: A, D
Página: 43

43. ¿Qué capa del modelo OSI proporciona la traducción de los datos?

A. Aplicación.
B. Presentación.
C. Sesión.
D. Transporte.
E. Enlace de datos.

Respuesta: B
Página: 42

44. ¿Cuál es el rango de números que determina una lista de acceso IPX extendida?

A. 100-199
B. 900-999
C. 1000-1999
D. 700-799

Respuesta: B
Página: 201

45. ¿Cuáles de las siguientes funciones pueden proporcionar los routers? (elija todas las que se apliquen).

A. División de dominios de colisión.
B. División de dominios de broadcast.
C. Direccionamiento lógico de redes.
D. Filtrado de direcciones físicas de la red local.

Respuesta: A, B, C, D
Página: 103

46. ¿Cuáles de las siguientes afirmaciones describen adecuadamente el protocolo de enrutamiento OSPF? (elija 2).

A. Soporta VLSM.
B. Se utiliza para enrutar entre sistemas autónomos.
C. Acota la inestabilidad de la red a una única área de la red.
D. Incrementa el tráfico de enrutamiento que circula en la red.
E. Permite un control amplio de las actualizaciones de enrutamiento.
F. Es más simple de configurar que RIPv2.

Respuesta: A, C, E
Página: 168

47. ¿En qué capa del modelo de tres capas de Cisco se utilizan típicamente los routers?

A. Acceso.
B. Principal.
C. Red.
D. Enlace de datos.
E. Distribución.

Respuesta: E
Página: 52

48. ¿Cuántos bits definen una dirección de hardware?

A. 6 bits.
B. 16 bits.
C. 46 bits.
D. 48 bits.

Respuesta: D
Página: 32

49. De las tecnologías enunciadas a continuación, ¿cuáles son las tres opciones que utilizan cable de cobre de par trenzado?

A. 100BaseFX
B. 100BaseTX
C. 100VG-AnyLAN
D. 10BaseT
E. 100BaseSX

Respuesta: B, C, D
Página: 25

100VG-AnyLAN es un medio de cobre muy antiguo casi en total desuso.

50. ¿Cuál es el resultado de segmentar una red con un puente?

A. Se aumenta el número de dominios de colisión.
B. Se reduce el número de dominios de colisión.
C. Se incrementa el número de dominios de broadcast.
D. Se reduce el número de dominios de broadcast.

Respuesta: A
Página: 218

51. ¿Cuáles de los siguientes son efectos de un porcentaje excesivo de colisiones en una LAN CSMA/CD? (elija 3).

A. Aumento del tráfico de broadcast.
B. Aumenta la latencia.
C. Baja el ancho de banda.
D. Aumenta el ancho de banda.
E. Aumenta la congestión.
F. Aumenta el ancho de banda disponible.

Respuesta: B, C, E
Página: 45

52. En un esfuerzo por incrementar la seguridad de su red WLAN, un técnico ha implementado WPA. ¿Qué dos definiciones pueden describir mejor el funcionamiento de WPA?.

A. Utiliza un método de autenticación abierta.
B. Especifica el uso de una encriptación pobre.
C. Incluye autenticaciones PSK
D. Utiliza una encriptación dinámica cuando el cliente establece conexión.
E. Requiere que todos los AP utilicen la misma encriptación.
F. WPA funciona solo con AP Cisco.

Respuesta: C, D
Página: 188

53. ¿Cuál es la dirección de subred de la dirección IP 192.168.100.30 / 255.255.255.248?

A. 192.168.100.32
B. 92.168.100.24
C. 192.168.100.0
D. 192.168.100.16

Respuesta: B
Página: 71

54. ¿Cuáles de estas afirmaciones contienen comparaciones válidas entre Fast Ethernet (100BaseTx) y Ethernet 10BaseT? (elija 4).

A. FastEthernet utiliza la misma Unidad Máxima de Transmisión (MTU) que Ethernet.
B. FastEthernet se basa en una extensión de la especificación IEEE 802.3.
C. FastEthernet funciona solamente en entornos full duplex, mientras que Ethernet puede operar tanto en half como full duplex.
D. FastEthernet utiliza el mismo método de control de acceso al medio (mecanismo MAC).
E. FastEthernet mantiene el formato de trama que utiliza Ethernet 10BaseT.
F. FastEthernet introduce modificaciones en el formato de la trama para lograr un mejor control del flujo de datos.
G. Fast Ethernet ofrece una velocidad 100 veces mayor que la de Ethernet 10BaseT.

Respuesta: A, B, D
Página: 43

55. Si el tamaño de la ventana de transmisión cambia de 3000 a 4000 durante la transferencia de datos de una sesión TCP, ¿qué puede hacer la terminal que está enviando?

A. Transmitir 3000 bytes antes de esperar por un acknowledgement.
B. Transmitir 4000 paquetes antes de esperar por un acknowledgement.
C. Transmitir 4000 bytes antes de esperar por un acknowledgement.
D. Transmitir 4000 segmentos antes de esperar por un acknowledgement.
E. Transmitir 3000 tramas antes de esperar por un acknowledgement.
F. Transmitir 3000 paquetes antes de esperar por un acknowledgement.

Respuesta: C
Página: 41

56. ¿Cuál de las siguientes es una lista de acceso IP extendida válida?

A. `access-list 110 permit ip any host 1.1.1.1 eq ftp`
B. `access-list 10 permit tcp ip any any eq 21`
C. `access-list 99 permit udp any host 2.2.2.2 eq ip`
D. `access-list 199 permit tcp any 0.0.0.0 255.255.255.255 eq 21`

Respuesta: D
Página: 202

57. ¿Cuál de los siguientes comandos mostrarán las interfaces que tienen aplicadas **ACL IP**?(elija2).

A. `show ip port`
B. `show access-lists`
C. `show ip interface`
D. `show access-lists interface`
E. `show running-config`

Respuesta: C, E
Página: 213

58. Convierta el número binario **10011101** en sus equivalentes decimal y hexadecimal.

¿Cuáles son los dos números correctos?

A. 159
B. 157
C. 185
D. 0x9d
E. 0xd9
F. 0x159

Respuesta: B,D
Página: 63

59. ¿Cuál es una desventaja de utilizar un protocolo orientado a la conexión como TCP?

A. La presencia de paquetes de acknowledgement puede agregar tráfico excedente.
B. Paquetes que no están marcados con el número de secuencia.
C. La pérdida o duplicación de paquetes de datos es más probable que ocurra.
D. La capa de aplicación debe asumir la responsabilidad de corregir la secuencia de los paquetes de datos.

Respuesta: A
Página: 41

60. ¿Qué capa del modelo Cisco de tres capas es la responsable de dividir los dominios de colisión?

A. Física.
B. Acceso.
C. Principal.
D. Red.
E. Distribución.
F. Enlace de datos.

Respuesta: B
Página: 52

61. De las siguientes opciones, ¿cuál le permite conectar directamente un PC a un router?

A. Conecte el puerto COM del PC al puerto consola del router utilizando un cable derecho.
B. Conecte el puerto COM del PC al puerto consola del router utilizando un cable cruzado.
C. Conecte el puerto COM del PC al puerto Ethernet del router utilizando un cable cruzado.
D. Conecte el puerto Ethernet del PC al puerto Ethernet del router utilizando un cable cruzado.
E. Conecte el puerto Ethernet del PC al puerto Ethernet del router utilizando un cable consola.
F. Conecte el puerto Ethernet del PC al puerto Ethernet del router utilizando un cable derecho.

Respuesta: D
Página: 28

62. ¿Cuál es la descripción adecuada de la capa de enlace de datos?

A. Esta capa segmenta y reensambla datos de una cadena de datos.
B. Esta capa administra direcciones de dispositivos, conoce la localización de los dispositivos en la red, y determina el mejor camino para mover los datos.
C. Esta capa transmite datos y maneja notificaciones de error, topología de la red y control de flujo.

Respuesta: C
Página: 30

63. La compañía ACME ha adquirido un nuevo switch para agregar a su red existente. Desean conectar este nuevo switch Ethernet a uno de los switches Ethernet ya existentes. ¿Qué cable debe ser utilizado para conectar los 2 switches entre sí?

A. Cable cruzado.
B. Cable directo.
C. Cable consola.
D. Cable de fibra.

Respuesta: A
Página: 28

64. Considere un circuito estándar Ethernet half-duplex. ¿Qué es verdadero respecto de este circuito?

A. Es una comunicación alternativa a través de una única vía.
B. El par receptor está conectado directamente al par transmisor de la estación remota.
C. El par transmisor está conectado directamente al par receptor de la estación remota.
D. No son posibles colisiones.
E. Ambas estaciones pueden transmitir simultáneamente.

Respuesta: A
Página: 43

65. ¿Cuál de las siguientes afirmaciones es verdadera respecto a una conexión confiable orientada a la transferencia de datos? (elija 2).

A. Se recibe una notificación de la recepción de los datos.
B. Cuando los buffers de memoria completan su capacidad, los datagramas son descartados y no se retransmiten.
C. Se utilizan "ventanas" para controlar la cantidad de información que se envía antes de recibir una confirmación de recepción.
D. Si expira el temporizador del segmento entre recepciones de confirmaciones, el nodo origen interrumpe la conexión.
E. El dispositivo destino espera por la confirmación desde el dispositivo origen antes de aceptar más datos.

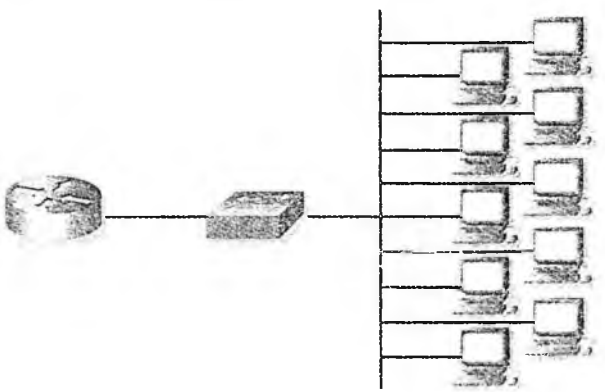
Respuesta: A, C
Página: 41

66. Juan se ha conectado a un PC en una subred remota vía telnet, ¿qué dirección MAC estará presente en la tabla ARP cuando ejecute en su terminal el comando arp –a?

A. Dirección MAC del puerto Ethernet del nodo destino.
B. Dirección MAC del puerto Ethernet del router local.
C. Dirección MAC del puerto serie del router de destino.
D. Dirección MAC del puerto serie del router local.

Respuesta: B
Página: 59, 60

67. Teniendo en cuenta la topología que se muestra en el gráfico. Cada nodo (se trata de 10 estaciones de trabajo) está conectado al switch a través de su propio puerto 10Mbps half-duplex, y a través de él a la interfaz E0 del router. ¿Cuál es el ancho de banda disponible para cada nodo?



A. 1 Mbps
B. 10 Mbps
C. 20 Mbps
D. 100 Mbps

Respuesta:

Al tratarse de una red conmutada, el ancho de banda se mantiene completo para cada conexión establecida (la interfaz del router es Ethernet, es decir, de 10 Mbps). Si se tratara de una red compartida (con un hub en lugar de un switch), el ancho de banda se distribuiría entre todos los nodos. El hecho de que sea half-duplex no cambia el ancho de banda disponible.

68. ¿Qué método de conmutación LAN ejecuta un CRC en cada trama?

A. Método de corte.
B. Almacenamiento y envío.
C. Verificación de fragmentos.
D. Libre de fragmentos.

Respuesta: B
Página: 219

69. ¿Qué tipo de conmutación LAN solo verifica la dirección de hardware de destino antes de enviar una trama?

A. Método de corte.
B. Almacenamiento y envío.
C. Verificación de Fragmentos.
D. Libre de Fragmentos.

Respuesta: A
Página: 219

70. ¿Qué significa el siguiente comando?

```
access-list 110 permit ip any 0.0.0.0 255.255.255.255
```

A. Es una lista de acceso IP estándar que permite solo la red 0.0.0.0
B. Es una lista de acceso IP extendida que permite solo la red 0.0.0.0
C. Es una lista de acceso IP extendida que permite a cualquier nodo o red.
D. Es inválido.

Respuesta: C
Página: 202

71. ¿Qué es verdadero respecto al estado de bloqueando de un puerto que está operando con el Protocolo de Árbol de Expansión (STP)? (elija 2).

A. No se transmiten o reciben tramas en un puerto que está bloqueando.
B. Se envían y reciben BPDU en un puerto que está bloqueando.
C. Aún se reciben BPDU en un puerto que está bloqueando.
D. Se envían o reciben tramas en un puerto que está bloqueando.

Respuesta: A, C
Página: 224

72. ¿Qué se utiliza para determinar el puente raíz en una red que corre el Protocolo de Árbol de Expansión (STP)? (elija 2 opciones).

A. Prioridad.
B. Coste de los enlaces conectados al switch.
C. Dirección MAC.
D. Dirección IP.

Respuesta: A, C
Página: 223

73. Unir cada estado del Protocolo de Árbol de Expansión con su definición correspondiente (STP).

Inicial
Aprendiendo
Escuchando
Enviando
Activo
Bloqueando

Completa la tabla de direcciones MAC pero no envía tramas de datos
Envía y recibe tramas de datos.
Prepara para enviar tramas de datos, sin aprender direcciones MAC
Previene el uso de rutas con bucles

Respuesta:

Los estados inicial y activo no existen. El estado bloqueando previene el uso rutas con bucles. En el estado de escuchando, el dispositivo se prepara para enviar datos verificando que no existan bucles, pero aún no ha comenzado a aprender direcciones MAC. En el estado de aprendiendo, comienza a poblar las tablas de direcciones MAC, pero aún no envía tramas de datos. Por último, en el estado de enviando, el puerto envía y recibe datos.

Página: 224

74. ¿Cuáles son las tres diferentes funciones que cumple un dispositivo de conmutación de capa 2?

A. Aprendizaje de direcciones.
B. Enrutamiento.

C. Envío y filtrado de tramas.
D. Crear bucles de red.
E. Evitar bucles de red.
F. Direccionamiento IP.

Respuesta: A, C, E
Página: 218

75. ¿Qué es verdadero respecto a las BPDU?

A. Se utilizan para enviar mensajes de configuración utilizando paquetes IP.
B. Se utilizan para enviar mensajes de configuración utilizando tramas multicast.
C. Se utilizan para determinar el coste de los enlaces STP.
D. Se utilizan para determinar la ID de puente de un switch.

Respuesta: B
Página: 222

76. Un nuevo switch ha sido comprado para actualizar la red. El objetivo del diseño de la red se centra en la eficiencia, y en privilegiar un transporte libre de errores por encima de la velocidad. ¿Qué modo del switch deberá configurar en el nuevo switch para proveer un transporte libre de errores a la red?

A. Método de corte
B. Libre de fragmentos
C. Filtrado de tramas
D. Almacenamiento y envío
E. Reenvío 802.1q
F. Modo VTP transparente

Respuesta: D
Página: 219

77. Si un switch determina que un puerto bloqueado debería ser ahora el puerto designado, ¿a qué estado pasará inmediatamente ese puerto?

A. Desbloqueado
B. Enviando
C. Escuchando
D. Escuchado

E. Aprendiendo
F. Aprendido

Respuesta: C
Página: 224

78. De las siguientes, ¿cuáles son dos afirmaciones verdaderas respecto del método de conmutación de almacenamiento y envío?

A. La latencia permanece constante, independientemente del tamaño de la trama.
B. La latencia al atravesar el switch varía de acuerdo al largo de la trama.
C. El switch recibe la trama completa antes de comenzar a reenviarlo.
D. El switch verifica la dirección de destino tan pronto como recibe el encabezado de la trama, y comienza a reenviarla inmediatamente.

Respuesta: B, C
Página: 219

79. ¿Cuál es la diferencia entre un puente y un switch de capa 2 o switch LAN? (elija 2).

A. Los puentes solo pueden tener una instancia de spanning-tree por puente.
B. Los switches pueden tener muchas instancias de spanning-tree por switch.
C. Los puentes pueden tener muchas instancias de spanning-tree por puente.
D. Los switches solo pueden tener una instancia de spanning-tree por switch.

Respuesta: A, B
Página: 223

80. ¿Cómo se denominan las Unidades de Datos de Protocolo en la capa de red del modelo OSI?

A. Principal.
B. Tramas.
C. Paquetes.
D. Segmentos.
E. Acceso.

F. Distribución.
G. Transporte.

Respuesta: C
Página: 49

81. Su gerente le pregunta sobre las características básicas de switches y hubs para brindar conectividad de red. ¿Qué le podría decir?

A. Los switches requieren menos tiempo que los hubs para procesar la trama.
B. Los switches no reenvían paquetes de difusión.
C. Los hubs pueden filtrar tramas.
D. El uso de hubs puede incrementar la cantidad de ancho de banda disponible para cada nodo.
E. Los switches incrementan el número de dominios de colisión en la red.

Respuesta: E
Página: 31

82. ¿Cuál es la diferencia entre un puente y un switch de capa 2? (elija 2 respuestas).

A. Los switches se basan en software.
B. Los puentes se basan en hardware.
C. Los switches se basan en hardware.
D. Los puentes se basan en software.

Respuesta: C, D
Página: 32

83. ¿Qué hace un switch cuando recibe una trama en una interfaz y la dirección de hardware de destino es desconocida o no figura en la tabla de filtrado de direcciones MAC?

A. Envía la trama al primer enlace disponible.
B. Deriva la trama a otro switch.
C. Inunda la red con la trama en busca del dispositivo de destino.
D. Envía un mensaje a la estación de origen pidiendo una resolución de nombre.

Respuesta: C
Página: 32

84. ¿Cómo se comunica el ID de un switch a los switches colindantes?

A. Enrutamiento IP.
B. STP.
C. Durante los cuatro estados STP de un switch.
D. Utilizando Unidades de Datos de Protocolo del Puente.
E. Difusión durante los tiempos de convergencia.

Respuesta: D
Página: 222

85. ¿Qué utiliza Frame-Relay para definir la tasa, en bits por segundo, a la que el switch Frame-Relay acuerda transferir datos?

A. Clock Rate (CR).
B. Committed Information Rate (CIR).
C. Local Management Interface (LMI).
D. Data-Link Connection Identifier (DLCI).
E. Committed Rate Measurement Interval (CRMI).

Respuesta: B
Página: 268

86. ¿Cuántos puentes raíz se permiten en un dominio de difusión?

A. 10
B. 1
C. Uno por cada switch
D. 20

Respuesta: B
Página: 223

87. ¿Qué podría ocurrir en una red si no se implementan tecnologías para prevenir los bucles en capa 2? (elija 2 respuestas).

A. Tiempos de convergencia más rápidos.
B. Tormentas de difusión.
C. Múltiples copias de una trama.
D. El enrutamiento IP ocasionará flapping (caídas variables) en un enlace serial.

Respuesta: B, C
Página: 222

88. ¿Cuál es la prioridad por defecto de un switch Cisco para el Protocolo de Árbol de Expansión?

A. 32.768
B. 3.276
C. 100
D. 10
E. 1

Respuesta: A
Página: 223

89. De las siguientes afirmaciones, ¿cuáles dos son verdaderas respecto de los puentes?

A. Un puente inunda tráfico multicast.
B. Un puente inunda tráfico de difusión.
C. Un puente no inunda tráfico multicast.
D. Un puente no inunda tráfico de difusión

Respuesta: A, B
Página: 31

90. ¿Cuál de las siguientes afirmaciones es verdadera respecto de puentes y switches? (elija 3).

A. Los switches están primariamente basados en software mientras que los puentes están basados en hardware.
B. Tanto puentes como switches reenvían el tráfico de difusión de capa 2.
C. Frecuentemente los puentes son más rápidos que los switches.
D. Los switches tienen un número de puertos mayor que la mayoría de los puentes.
E. Los puentes definen dominios de difusión mientras que los switches definen dominios de colisión.
F. Puentes y switches toman decisiones de reenvío basados en el direccionamiento de capa 2.

Respuesta: B, D, F
Página: 31

91. ¿Cuál de las siguientes opciones es verdadera? (elija todas las que se apliquen).

A. PPP puede utilizarse con Token Ring.
B. PPP puede utilizarse con enlaces en serie síncronos.
C. PPP puede utilizarse con enlaces en serie asíncronos.
D. PPP es propiedad del equipamiento de cada vendedor.

Respuesta: B, C
Página: 257

92. ¿Qué métodos de conmutación LAN tienen un tiempo de latencia fijo? (elija todos los que se apliquen).

A. Método de corte.
B. Almacenamiento y envío.
C. Verificación de fragmentos.
D. Libre de fragmentos.

Respuesta: A, D
Página: 219

93. ¿Qué indica el término "Base" en "10BaseT"?

A. Cableado de backbone que utiliza muchas señales digitales al mismo tiempo en un único cable.
B. Cableado de banda base que utiliza muchas señales digitales al mismo tiempo en un único cable.
C. Cableado de backbone que utiliza solo una señal digital a la vez en el cable.
D. Cableado de banda base que utiliza solo una señal digital a la vez en el cable.

Respuesta: D
Página: 24

94. ¿Qué es verdadero respecto a Frame-Relay DLCI?

A. DLCI es opcional en una red Frame-Relay.
B. DLCI representa a un único circuito físico.
C. DLCI identifica una conexión lógica entre dispositivos DTE.
D. DLCI se utiliza para etiquetar el principio de una trama cuando se utiliza la conmutación LAN.

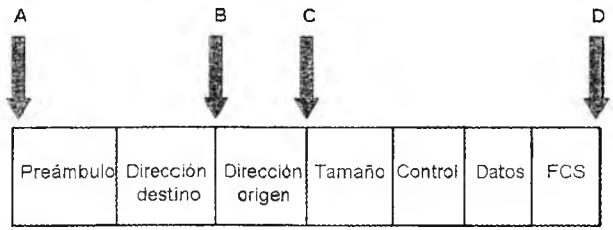
Respuesta: C
Página: 268

95. Durante la encapsulación, ¿en qué orden es empaquetada la información?

A. Datos, paquete, segmento, trama
B. Segmento, datos, paquete, trama
C. Datos, segmento, paquete, trama
D. Paquete, datos, segmento, trama

Respuesta: C
Página: 50

96. ¿En qué punto de la trama que se muestra en el diagrama se toma la decisión de conmutación en la modalidad almacenamiento y envío?



A. A
B. B
C. C
D. D

Respuesta: D
Página: 219

97. El Protocolo de Árbol de Expansión fue originalmente desarrollado por DEC. ¿Por qué razón se utiliza STP en las redes LAN conmutadas?

A. Para proveer un mecanismo para el monitoreo de la red en entornos conmutados.
B. Para preveer los bucles de enrutamiento en redes conmutadas con caminos redundantes.
C. Para administrar el agregado, eliminación y nombrado de VLAN a través de múltiples switches.
D. Para segmentar una red en múltiples dominios de colisión.

Respuesta: B
Página: 222

98. ¿Cuál de las siguientes afirmaciones es verdadera acerca de las VLAN?

A. Se deben tener al menos dos VLAN definidas en cada red conmutada.
B. Todas las VLAN se configuran en el switch más rápido y, por defecto, se propaga esta información a los demás switches.
C. No deberían tenerse más que 10 switches en el mismo dominio VTP.
D. VTP se utiliza para enviar información de las VLAN a todos los switches en un dominio
E. VTP configurado.

Respuesta: D
Página: 229

99. ¿Cuáles de las siguientes son características únicas de Ethernet half-duplex comparada con Ethernet full-duplex? (elija 2).

A. Comparte el dominio de colisión.
B. Genera dominios de colisión únicos.
C. Aumenta el throughput efectivo.
D. Reduce el throughput efectivo.
E. Genera dominios de difusión únicos.

Respuesta: A, C
Página: 43

100. ¿Qué wildcard utilizaría para filtrar el siguiente conjunto de redes?

172.16.32.0 a **172.16.63.0**

A. 172.16.0.0 0.0.0.255
B. 172.16.255.255 0.0.0.0
C. 0.0.0.0 255.255.255.255
D. 172.16.32.0 0.0.0.255
E. 172.16.32.0 0.0.0.31
F. 172.16.32.0 0.0.31.255
G. 172.16.32.0 0.31.255.255
H. 172.16.32.0 0.0.63.255

Respuesta: F
Página: 199

101. ¿Cuáles son las dos formas en las cuales un administrador puede configurar las VLAN?

A. A través de un servidor DHCP.
B. Estáticamente.
C. Dinámicamente.
D. A través de una base de datos VTP.

Respuesta: B, C
Página: 225

102. ¿Qué tamaño de trama máximo es posible sobre un enlace troncal que encapsula Ethernet con ISL?

A. 1518
B. 1548
C. 4202
D. 8190

Respuesta: B
Página: 228

Una trama ISL encapsulando tráfico Ethernet puede tener una longitud de hasta 1548 bytes. Una trama Ethernet puede transmitir hasta 1500 bytes de datos; si se consideran los encabezados Ethernet, la longitud total es de 1518 bytes. Si se trata de una trama Ethernet encapsulada sobre ISL, la longitud máxima total puede ser de hasta 1548 bytes ya que ISL agrega 30 bytes a la trama original.

103. ¿Cómo se configuran las VLAN dinámicas?

A. Estáticamente
B. A través de un operador on-line
C. A través de un servidor DHCP
D. A través de un servidor de pertenecía de VLAN (VMPS)

Respuesta: D
Página: 240

104. ¿Cuáles de los siguientes protocolos se utilizan cuando se configura el puerto troncal de un switch? (elija 2).

A. Protocolo Troncal Virtual (VTP)
B. VLAN

C. 802.1q
D. ISL

Respuesta: C, D
Página: 227

105. ¿Cuál de las siguientes afirmaciones es verdadera respecto a VTP? (elija 2).

A. El recorte VTP se habilita por defecto en todos los switches.
B. El recorte VTP está inhabilitado por defecto en todos los switches.
C. Solo se puede ejecutar el recorte VTP en switches 5000 o superiores.
D. El recorte VTP se configura en todos los switches por defecto si se activa en solo el switch que es servidor VTP.

Respuesta: B, D
Página: 232

106. Usted trabaja como técnico de la red de una compañía y se le ha encomendado agregar un nuevo router en una red OSPF ya establecida. La red directamente conectada al router que se agregó con el nuevo router no aparece en las tablas de enrutamiento de los demás routers OSPF. Contando con la información parcial de la configuración que se muestra abajo, ¿cuál es el error de configuración que está causando problemas?

```
Router(config)#router ospf 1
Router(config-router)#network 10.10.10.0 255.0.0.0 area 0
```

A. El sistema autónomo no está correctamente configurado.
B. La máscara de subred de la red está incorrectamente configurada.
C. La máscara de wildcard de la red está configurada incorrectamente.
D. El número de red no está correctamente configurado.
E. El identificador de proceso está configurado incorrectamente.

Respuesta: C
Página: 172, 175

107. ¿Cuál de los siguientes encapsula una trama y le agrega un nuevo campo FCS?

A. ISL
B. 802.1q
C. 802.1x

D. 802.3u

Respuesta: A
Página: 227

108. Si su red Frame-Relay se encuentra congestionada, ¿qué mecanismo utiliza para indicarle al dispositivo de origen que reduzca la velocidad de envío?

A. HDLC.
B. DLCI.
C. FECN.
D. BECN.

Respuesta: D
Página: 269

109. ¿Qué se logra al configurar en un switch el modo VTP transparente?

A. El switch en modo transparente solo enviará mensajes y publicaciones sin agregarlos a su propia base de datos.
B. El switch en modo transparente enviará mensajes y publicaciones y además los agregará a su propia base de datos.
C. El switch en modo transparente no enviará mensajes y publicaciones.
D. El modo transparente hace a un switch dinámicamente seguro.

Respuesta: A
Página: 231

110. ¿Cuál de los siguientes enunciados representa beneficios que proporciona VTP a una red conmutada? (elija 6).

A. Dominios de difusión múltiples en VLAN 1.
B. Administración de todos los switches y routers de una red.
C. Consistencia de la configuración VLAN a través de todos los switches de la red.
D. Permitir que las VLAN puedan ser convertidas en troncales a través de redes mezcladas, tales como Ethernet a ATM LANE o FDDI.
E. Rastreo y monitoreo precisos de las VLAN.
F. Informes dinámicos de VLAN agregadas a todos los switches.
G. Agregar VLAN de modo plug-and-play.
H. Configuración automática de VLAN.

Respuesta: A, C, D, E, F, G
Página: 229

111. Se adquirió un router usado y no logra ingresar al modo privilegiado porque el router tiene configurada una contraseña. Necesita realizar entonces un procedimiento de recuperación de contraseña. El primer paso en este procedimiento es revisar los valores actuales del registro de configuración desde el modo usuario. ¿Cuál es el comando que le permitirá ver el registro de configuración desde el modo usuario?

A. `show register`
B. `show flash`
C. `show boot`
D. `show version`

Respuesta: D
Página: 129

112. ¿Cuál de las siguientes afirmaciones es verdadera respecto a VTP?

A. Todos los switches son servidores VTP por defecto.
B. Todos los switches son VTP transparente por defecto.
C. VTP está activo por defecto con un nombre de dominio preestablecido en todos los switches.
D. Todos los switches son clientes VTP por defecto.

Respuesta: A
Página: 229

113. ¿Qué utiliza el protocolo ISL para identificar la membresía de VLAN de una trama sobre un enlace troncal?

A. Filtrado de tramas con VLAN ID.
B. Marcado de tramas con VLAN ID.
C. Filtrado de tramas con ID de troncal.
D. Marcado de tramas con ID de troncal.
E. Filtrado de tramas con ID de puerto VTP.

Respuesta: B
Página: 227

114. ¿Qué es un puerto troncal?

A. Un puerto que es parte de solo una VLAN y a la que se denomina VLAN nativa del puerto.
B. Un puerto que puede transportar múltiples VLAN.

C. Un puerto de switch conectado a Internet.
D. Capacidad para datos y voz en la misma interfaz.

Respuesta: B
Página: 226

115. ¿Qué es un puerto de acceso?

A. Un puerto que es parte de solo una VLAN, que se denomina VLAN nativa del puerto.
B. Un puerto que puede transportar múltiples VLAN.
C. Un puerto de switch conectado a Internet.
D. Capacidad para datos y voz en la misma interfaz.

Respuesta: E
Página: 226

116. ¿Qué hace una VLAN?

A. Divide dominios de colisión
B. Divide dominios de enrutamiento
C. Divide dominios de difusión (broadcast)
D. Proporciona segmentación de la fragmentación

Respuesta: C
Página: 225, 226

117. ¿Cuál de las siguientes afirmaciones es verdadera respecto a los enlaces troncales?

A. Están configurados por defecto en todos los puertos del switch.
B. Solo funcionan con un tipo de red Ethernet y no con Token Ring, FDDI, o ATM.
C. Se pueden configurar enlaces troncales en cualquier puerto de 10, 100 y 1000 Mbps.
D. Debe retirar manualmente aquellas VLAN que no quiere que circulen por el troncal.

Respuesta: D
Página: 226, 232

118. ¿Cuándo actualizará un switch su base de datos VTP?

A. Cada 60 segundos.

B. Cuando un switch recibe una publicación que tiene un número de revisión más alto, el switch sobrescribirá la base de datos que guarda en la NVRAM con la nueva base de datos que está siendo publicada.
C. Cuando un switch hace difusión de una publicación que tenga un número de revisión más bajo, el switch sobrescribirá la base de datos que guarda en la NVRAM con la nueva base de datos que está siendo publicada.
D. Cuando un switch recibe una publicación que tiene el mismo número de revisión, el switch sobrescribirá la base de datos que guarda en la NVRAM con la nueva base de datos que está siendo publicada.

Respuesta: B
Página: 231

119. ¿Cuál de los que se enuncia a continuación es un estándar IEEE para el etiquetado de tramas?

A. ISL
B. 802.3z
C. 802.1q
D. 802.3u

Respuesta: C
Página: 227

120. ¿Cuál de los siguientes enunciados describe correctamente un enlace troncal? (elija 2 respuestas).

A. Pueden transportar simultáneamente múltiples VLAN.
B. Los switches borran cualquier información acerca de la VLAN contenida en la trama antes de ser enviada a un dispositivo a través de un puerto de acceso.
C. Los dispositivos conectados a puertos de acceso no pueden comunicarse con dispositivos fuera de su VLAN a menos que el paquete se enrute a través de un router.
D. Los puertos troncales se utilizan para transportar tráfico de una o varias VLAN entre dispositivos que pueden configurarse para transportar a todas las VLAN o solo a algunas.

Respuesta: A, D
Página: 226

121. ¿Cuál de las siguientes afirmaciones es verdadera respecto a un puerto de acceso? (elija 2).

A. Pueden transportar simultáneamente múltiples VLAN.
B. Los switches borran cualquier información de la VLAN contenida en la trama antes de que esta sea enviada a un dispositivo a través de un puerto de acceso.
C. Los dispositivos conectados a puertos de acceso no pueden comunicarse con dispositivos fuera de su VLAN a menos que el paquete se enrute a través de un router.
D. Los puertos de acceso se utilizan para transportar las VLAN entre dispositivos y pueden configurarse para transportar a todas las VLAN o solo a algunas.

Respuesta: B, C
Página: 227, 243

122. ¿Cuál de los siguientes enunciados describe correctamente los enlaces de acceso?

A. Pueden transportar múltiples VLAN.
B. Se utilizan para transportar VLAN entre dispositivos y pueden configurarse para transportar a todas las VLAN o solo algunas.
C. Solo se pueden utilizar con FastEthernet o Gigabit Ethernet.
D. Son parte de solo una VLAN y se la denomina VLAN nativa del puerto.

Respuesta: D
Página: 226

123. ¿Cuál es el método IEEE de etiquetado de tramas?

A. ISL
B. LANE
C. Campo SAID
D. 802.1Q

Respuesta: D
Página: 227

124. Usted trabaja como técnico de red. Ha completado el proceso de recuperación de claves en un router Cisco. El procedimiento ha sido exitoso y el router retorna a su operación normal. ¿Cuál es el valor del registro de configuración en este momento?

A. 0x2100
B. 0x2101
C. 0x2102
D. 0x2124
E. 0x2142

Respuesta: C
Página: 132

125. ¿Qué modo VTP no participa en el dominio VTP pero aún así enviará publicaciones VTP a través de los enlaces troncales configurados?

A. ISL.
B. Cliente.
C. Transparente.
D. Servidor.

Respuesta: C
Página: 231

126. ¿Cuál es el tamaño de un encabezado ISL?

A. 4 bytes.
B. 6 bytes.
C. 26 bytes.
D. 1522 bytes.

Respuesta: C
Página: 227, 228

127. ¿En qué momento el switch utiliza la técnica de etiquetado de tramas?

A. Cuando las VLAN están atravesando un puerto de acceso.
B. Cuando las VLAN están atravesando un puerto troncal.
C. Cuando se utiliza ISL en un puerto de acceso.
D. Cuando se utiliza 802.1Q en un puerto de acceso.

Respuesta: B
Página: 227

128. La compañía ABC acaba de convocarlo como consultor para agregar una nueva VLAN denominada "ventas" a la red conmutada existente.

¿Cuales de las siguientes afirmaciones son verdaderas respecto al proceso de configuración de esta nueva VLAN? (elija 3).

A. La VLAN debe ser creada.
B. La VLAN debe ser nombrada.
C. Una dirección IP debe ser configurada para la VLAN.
D. Los puertos seleccionados deben ser agregados a la nueva VLAN.
E. La VLAN debe ser agregada al dominio STP.

Respuesta: A, B, D
Página: 241

129. Su compañía utiliza un switch para dar acceso a la red de su Departamento de Capacitación. Necesita realizar cambios en ese switch de modo remoto, de manera tal que pueda habilitar a diferentes aulas a tener acceso a Internet según sea necesario.

¿Qué deberá configurar en este switch para que pueda hacer estos cambios remotamente? (seleccione 2).

A. El nombre del switch deberá coincidir con el nombre del grupo de trabajo de la red local.
B. Se deberá configurar una dirección IP y un default gateway en el switch.
C. La estación de trabajo remota desde la que se configure deberá tener acceso a través de la VLAN de administración del switch.
D. CDP debe estar habilitado en el switch de modo tal que otros dispositivos presentes en la red puedan localizarlo.

Respuesta: B, C
Página: 236

130. ¿Cuál de los siguientes comandos configurará una interfaz de un switch para transportar tráfico de todas las VLAN hacia otro switch directamente conectado?

A. `Sw(config-if)#vlan all`
B. `Sw(config-if)#switchport trunk encapsulation dot1q`
C. `Sw(config-if)#switchport access vlan full`

D. `Sw(config-if)#switchport mode trunk`
E. `Sw(config-if)#switchport access vlan 30`

Respuesta: D
Página: 243

131. ¿En cuál de los siguientes modos de la interfaz de línea de comandos debe ubicarse para ejecutar el comando que permite borrar la configuración inicial del switch?

A. Modo usuario.
B. Modo privilegiado.
C. Modo inicial.
D. Modo configuración global.
E. Modo configuración de la interfaz.

Respuesta: B
Página: 124

132. ¿En qué modo puede usted configurar la opción de full-duplex para la interfaz fastethernet0/5?

A. Modo usuario.
B. Modo privilegiado.
C. Modo inicial.
D. Modo configuración global.
E. Modo configuración de la interfaz.

Respuesta: E
Página: 238

133. El comando **show interface vlan 1** muestra:

A. La versión de software de la VLAN 1.
B. La configuración de la dirección IP.
C. Los puertos del switch actualmente miembros de todas la VLAN.
D. Las opciones de seguridad de la VLAN.

Respuesta: B
Página: 237

134. Un switch tiene un PC conectado a la interfaz fastethernet 0/1 y un router a la interfaz fastethernet 0/2. El PC necesita utilizar TCP/IP para comunicarse a través del router con otros nodos TCP/IP. ¿En qué modo de configuración podrá usted configurar la dirección IP del switch?

A. Modo usuario.
B. Modo privilegiado.
C. Modo inicial.
D. Modo configuración global.
E. Modo configuración de la interfaz para cada una de las interfaces mencionadas.
F. Ninguna de las anteriores.

Respuesta: F
Página: 236

135. Esta es la salida de consola de un switch. ¿Cuál es la función de este switch?

```
Switch#show vtp status
VTP versión: 2
Configuration Revision: 0
Maximum VLANs supported locally: 64
Number of existing VLANs: 5
VTP Operating Mode: Client
VTP Domain Name: Salta
VTP Prunning Mode: Disabled
VTP V2 Mode: Disabled
VTP Traps Generation Disabled
```

A. Aprender y guardar configuraciones VTP en su configuración activa.
B. Crear y modificar VLAN.
C. Recibir información sobre configuraciones VTP.
D. VTP está deshabilitado en este dispositivo.
E. VTP no está guardado en la NVRAM.

Respuesta: C
Página: 231, 249

136. En el siguiente comando, ¿qué significa el número 175?

```
ip route 150.150.0.0 255.255.0.0 150.150.150.150 175
```

A. Define el siguiente salto

B. Define la distancia administrativa
C. Significa que la actualización se ha enviado como broadcast
D. Nada, es un comando inválido

Respuesta: B
Página: 89

137. ¿Qué comando se puede ejecutar en la interfaz para indicarle al switch que ponga la interfaz nuevamente en servicio?

A. `up`
B. `admin up`
C. `no shutdown`
D. `no admin shutdown`
E. `enable`

Respuesta: C
Página: 238, 245

138. ¿Qué comando muestra información acerca de la versión de software en un switch?

A. `display version`
B. `show version`
C. `show ios`
D. `show software version`

Respuesta: B
Página: 129, 130

139. ¿Cuál de los siguientes comandos permite configurar la dirección IP del default gateway del switch?

A. `switch(conf)#ip default gateway [address]`
B. `switch(conf)#ip default-gateway [address]`
C. `switch(conf)#ip gateway default [address]`
D. `switch(conf)#ip-default-gateway [address]`

Respuesta: B
Página: 236, 237

140. ¿Cuál de los siguientes comandos se requiere para crear un enlace 802.1Q en un switch basado en IOS cuando se desea establecer un enlace troncal entre 2 switches? (elija 2)

A. `Switch(vlan)#mode trunk`
B. `Switch(config)#switchport access mode trunk`
C. `Switch(config-if)#switchport mode trunk`
D. `Switch(config-if)#switchport trunk encapsulation dot1q`
E. `Switch(config)#switchport access mode 1`
F. `Switch(vlan)#trunk encapsulation dot1q`

Respuesta: C, D
Página: 243

141. Un técnico ha instalado un nuevo AP IEEE 802.11b en su red wireless. ¿Cuál es el máximo de velocidad de transmisión del AP?

A. 11 mbps
B. 100 mbps
C. 54 mbps
D. 10 mbps
E. 1000 mbps
F. 16 mbps
G. Ninguna de las anteriores

Respuesta: A
Página: 180

142. ¿Qué comando se utiliza en un switch para configurar la dirección IP del switch para poder realizar administración por red a la dirección 10.1.1.1, máscara de subred 255.255.255.0?

A. `ip addess 10.1.1.1 255.255.255.0`
B. `ip 10.1.1.1 255.255.255.0`
C. `address 10.1.1.1 255.255.255.0`
D. `set ip address 10.1.1.1 255.255.255.0`
E. `ip address 10.1.1.1 mask 255.255.255.0`

Respuesta: A
Página: 236

143. ¿Qué hace un switch con una trama multicast recibida en una interfaz?

A. Envía la trama al primer puerto disponible.
B. Descarta la trama.
C. Inunda la red con la trama buscando el dispositivo.
D. Devuelve un mensaje a la estación origen pidiendo una resolución de nombre.

Respuesta: C
Página: 219

144. ¿Qué comando IOS copia la configuración de la RAM a la NVRAM?

A. `copy running-config ftp`
B. `copy tftp running-config`
C. `copy running-config Stara-up-config`
D. `copy start-up-config running-config`
E. `copy startup-config running-config`
F. `copy running-config startup-config`

Respuesta: F
Página: 124

145. ¿Cuál de los siguientes comandos del modo configuración de interfaz establece la velocidad de una interfaz?

A. `port speed 10`
B. `speed 10`
C. `outbound speed 100 auto`
D. `inbound speed 100 auto`
E. `duplex full`

Respuesta: B
Página: 238

146. ¿Cuál de los siguientes comandos reinicia todo el software y hardware de un switch?

A. `reboot`
B. `reload`
C. `reconfig`
D. `configure terminal`

Respuesta: B
Página: 126

147. ¿Cuáles son los dos comandos que puede utilizar para verificar la configuración que será utilizada cuando reinicia nuevamente el switch?

A. `show config`
B. `show startup-config`
C. `show running-config`
D. `show version`

148. ¿Qué protocolo que funciona en la capa de transporte proporciona un servicio no orientado a la conexión entre nodos?

A. IP.
B. ARP.
C. TCP.
D. UDP.

Respuesta: D
Página: 42

149. ¿Qué protocolo funciona en la capa de transporte y proporciona circuitos virtuales entre nodos?

A. IP.
B. ARP.
C. TCP.
D. UDP.

Respuesta: C
Página: 42

150. ¿Qué protocolo funciona en la capa de Internet y proporciona un servicio no orientado a la conexión entre nodos?

A. IP.
B. ARP.
C. TCP.
D. UDP.

Respuesta: A
Página: 58

151. Si un nodo hace difusión de una trama que incluye una dirección de hardware de origen y destino, y su propósito es obtener una dirección IP para sí mismo, ¿qué protocolo de la capa de red utiliza el nodo?

A. RARP.
B. ARPA.
C. ICMP.
D. TCP.
E. IPX.

Respuesta: A
Página: 58

152. Si una interfaz de router está congestionada, ¿qué protocolo de la suite IP se utiliza para comunicar esta situación a los routers colindantes?

A. RARP.
B. ARP.
C. ICMP.
D. IP.
E. TCP.

Respuesta: C
Página: 58

153. ¿De cuántos bytes es una dirección Ethernet?

A. 3
B. 4
C. 5
D. 6
E. 7
F. 8
G. 48

Respuesta: D
Página: 32

154. ¿Cuál de las siguientes afirmaciones corresponde a características típicas de la implementación de VLAN? (elija 3)

A. Las VLAN dividen lógicamente un switch de modo que operativamente, a nivel de capa 2, se obtienen múltiples switches independientes entre sí.
B. Una VLAN puede atravesar múltiples switches.
C. Las VLAN típicamente disminuyen el número de dominios de difusión.
D. Un enlace troncal puede conducir tráfico de múltiples VLAN.
E. La implementación de VLAN incrementa significativamente el tráfico en una red porque la información del troncal debe ser agregada en cada paquete.
F. Las VLAN extienden los dominios de colisión para incluir múltiples switches.

Respuesta: A, B, D
Página: 225, 226

155. ¿Qué protocolo se utiliza en un entorno IP para obtener la dirección de hardware de un dispositivo local destino?

A. RARP.
B. ARP.
C. IP.
D. ICMP.
E. BootP.

Respuesta: B
Página: 58

156. ¿Cuál es el tiempo típico que requiere un puerto de switch para pasar del estado de bloqueando al de enviando?

A. 5 segundos.
B. 50 segundos.
C. 10 segundos.
D. 100 segundos.

Respuesta: B
Página: 225

157. ¿Qué clase de dirección IP proporciona un máximo de solo 254 direcciones de nodo disponibles por ID de red?

A. Clase A.
B. Clase B.
C. Clase C.
D. Clase D.
E. Clase E.

Respuesta: C
Página: 68

158. ¿Cuáles de los siguientes rangos se consideran números de puerto bien conocidos?

A. 1-1023.
B. 1024 y superiores.
C. 1-256.
D. 1-65534.

159. ¿Qué protocolo utiliza una red Ethernet para verificar una dirección IP a partir de una dirección Ethernet conocida?

A. IP.
B. ARP.
C. RARP.
D. TCP.

Respuesta: C
Página: 58

160. ¿Qué dos comandos le permiten verificar la configuración de direcciones IP en su red?

A. `ping`
B. `traceroute`
C. `verify`
D. `test IP`
E. `echo IP`
F. `config IP`

Respuesta: A, B
Página: 140

161. ¿Cuáles de las siguientes son dos características del protocolo RARP?

A. Genera mensajes con indicaciones de problemas.
B. Mapea direcciones IP a direcciones Ethernet.
C. Mapea direcciones Ethernet a direcciones IP.
D. Está implementado directamente por encima de la capa de enlace de datos.

Respuesta: C, D
Página: 58

162. Usted quiere agregar a su WLAN un nuevo punto de acceso. ¿Qué configuración adicional es necesaria si ya tiene configurado el SSID en el AP?

A. Configurar una autenticación abierta en el AP y en el cliente.
B. Configurar el SSID con los valores predeterminados.
C. Configurar el SSID en el con los parámetros del SSID del AP.
D. Configurar la MAC permitiendo al cliente conectarse al AP.
E. Todas las anteriores son correctas.

Respuesta: C, D, E
Página: 190

163. ¿Qué tipo de dirección es la siguiente?:

172.16.0.254 máscara 255.255.0.0

A. IPX, dirección MAC.
B. IP, dirección de difusión clase C.
C. Dirección IP privada, dirección de un nodo.
D. Dirección IP pública, dirección de difusión.
E. Dirección IP privada, dirección de difusión.

Respuesta: C
Página: 71

164. ¿Qué comandos pueden ser utilizados en la interfaz de línea de comandos para diagnosticar problemas de conectividad a nivel de capa de red en un router? (seleccione 3).

A. `ping`
B. `traceroute`
C. `ipconfig`
D. `show ip route`
E. `winipcfg`
F. `show controllers`

Respuesta: A, B, D
Página: 140, 143

165. En el esquema jerárquico de direccionamiento IP, ¿qué establece que porción de una dirección IP identifica el número de red y cuál el nodo?

A. Máscara de subred.
B. Puntos entre los octetos.
C. Numeración del primer octeto.
D. Asignación de DHCP.
E. ARP.

Respuesta: A
Página: 71

166. La dirección IP 131.107.0.0 es una dirección clase B. ¿Cuál es el rango de valores binarios para el primer octeto de las direcciones de esta clase?

A. 10000000 a 11111111
B. 00000000 a 10111111
C. 10000000 a 10111111
D. 10000000 a 11011111
E. 11000000 a 11101111

Respuesta: C
Página: 71, 77

167. Los usuarios de la red 192.168.69.0/28 no pueden acceder al servidor de la Intranet corporativa en la dirección www.inhouse.com. Al diagnosticar este problema, encuentra que puede conectarse por telnet desde terminales de su red al webserver vía su dirección IP. ¿Cuál es probablemente la causa de este problema?

A. Fallo de TCP/IP.
B. Fallo de DNS.
C. Fallo de FTP.
D. Fallo de SNMP.

Respuesta: B
Página: 56

168. Un administrador está diagnosticando posibles problemas en su red, para lo cual ha ejecutado el comando ping 10.0.0.2 para probar la conectividad física entre 2 dispositivos. ¿Qué tipo de mensaje ICMP ha sido transportado en el datagrama IP?

A. ICMP echo.
B. Information request.
C. Timestamp reply.
D. ICMP Redirect.
E. Source quench.

Respuesta: A
Página: 141

169. No se logra conectar al servidor TFTP local de la compañía utilizando la dirección IP 10.0.0.20 desde su terminal. Desea probar su terminal para estar seguro de que TCP/IP está correctamente instalado.

¿Cuál de las siguientes acciones le permite probar la suite de protocolos en su PC?

A. ping 127.0.0.0
B. ping 203.125.12.1
C. telnet 127.0.0.1
D. ping 127.0.0.1
E. tracert 203.125.12.1

Respuesta: D
Página: 69

170. ¿Cuál de las siguientes opciones no implementaría en la capa de distribución?

A. Listas de acceso.
B. Filtrado de paquetes.
C. Cola.
D. División de dominios de colisión.
E. Traducción de la dirección.
F. , Firewalls.
G. División de dominios de difusión.

Respuesta: D
Página: 52

171. ¿Cuál es la longitud máxima admitida para un cable de par trenzado en una red FastEthernet 100BaseTX estándar?

A. 10 m.
B. 50 m.
C. 100 m.
D. 1000 m.

Respuesta: C
Página: 25

172. ¿Cuál es la dirección de broadcast de la dirección de subred 192.168.99.20 255.255.255.252?

A. 192.168.99.127
B. 192.168.99.63
C. 192.168.99.23
D. 192.168.99.31

Respuesta: C
Página: 71

173. ¿Cómo se determina el puerto raíz de un switch que está corriendo el Protocolo de Árbol de Expansión?

A. El switch determina el coste más alto de un enlace al puente raíz.
B. El switch determina el coste más bajo de un enlace al puente raíz.
C. La tasa de transferencia BPDU más rápida se determina enviando y recibiendo BPDU entre switches, y esa interfaz se convierte en el puerto raíz.
D. El puente raíz efectuará una difusión del ID del puente, y el puente receptor determinará en qué interfaz fue recibido esta difusión y convertirá a dicha interfaz en el puerto raíz.

Respuesta: B
Página: 223

174. ¿Cuál es el rango de nodo válido del cual es parte la dirección IP 172.16.10.22 255.255.255.240?

A. 172.16.10.20 a 172.16.10.22
B. 172.16.10.1 a 172.16.10.255
C. 172.16.1.16 a 172.16.10.23
D. 172.16.10.17 a 172.16.10.31
E. 172.16.10.17 a 172.16.10.30

Respuesta: E
Página: 71

175. ¿Cuál es el rango de números de puerto que un cliente puede utilizar para configurar una sesión con otro nodo o un servidor?

A. 1-1023.
B. 1024 y superiores.
C. 1-256.
D. 1-65534.

Respuesta: B
Página: 40

176. Un usuario ejecuta el comando **ping 204.211.38.52** durante una sesión de consola en un router. ¿Qué está utilizando este comando para verificar la conectividad entre los dos dispositivos?

A. ICMP echo request.
B. Information request.
C. Timestamp reply.

D. Redirect.
E. Source quench.

Respuesta: A
Página: 140

177. ¿Cuál de las siguientes es la dirección de difusión para una ID de red Clase B que utiliza la máscara de subred por defecto?

A. 172.16.10.255
B. 172.16.255.255
C. 172.255.255.254
D. 255.255.255.255

Respuesta: B
Página: 71

178. Desde el prompt DOS de una estación de trabajo puede hacer ping a un router pero no puede hacer telnet al mismo. ¿Cuál es la causa más probable del problema?

A. El PC tiene una placa de red defectuosa.
B. La dirección IP del router está en una subred diferente.
C. No se ha configurado la password de terminal virtual en el router.
D. No se ha configurado el default gateway en el PC.
E. La dirección IP del terminal es incorrecta.

Respuesta: C
Página: 113

179. ¿Cuál es la dirección de difusión que corresponde a la IP 10.254.255.19 255.255.255.248?

A. 10.254.255.23
B. 10.254.255.24
C. 10.254.255.255
D. 10.255.255.255

Respuesta: A
Página: 71

180. ¿Qué es verdadero respecto al estado de bloqueando de un puerto de switch que utiliza el Protocolo de Árbol de Expansión? (elija todas las respuestas que se apliquen).

A. Los puertos bloqueados no envían ninguna trama.
B. Los puertos bloqueados escuchan BPDU.
C. Los puertos bloqueados envían todas las tramas.
D. Los puertos bloqueados no escuchan BPDU.

Respuesta: A, B
Página: 224

181. ¿Cuál es la dirección de difusión de la dirección de subred 172.16.99.99 / 255.255.192.0?

A. 172.16.99.255
B. 172.16.127.255
C. 172.16.255.255
D. 172.16.64.127

Respuesta: B
Página: 71

182. Si usted deseara tener 12 subredes con un ID de red Clase C, ¿qué máscara de subred debería utilizar?

A. 255.255.255.252
B. 255.255.255.248
C. 255.255.255.240
D. 255.255.255.255

Respuesta: C
Página: 71

183. ¿Cuál es la dirección de difusión de la subred a la que pertenece el puerto 10.10.10.10 255.255.254.0?

A. 10.10.10.255
B. 10.10.11.255
C. 10.10.255.255
D. 10.255.255.255

Respuesta: B
Página: 71

184. A partir de la red 199.141.27.0 con una máscara de subred 255.255.255.240, identifique las direcciones de nodo válidas (elija 3).

A. 199.141.27.33
B. 199.141.27.112

C. 199.141.27.119
D. 199.141.27.126
E. 199.141.27.175
F. 199.141.27.208

Respuesta: B, D, E
Página: 71

185. La red 172.12.0.0 necesita ser dividida en subredes, cada una de las cuales debe tener una capacidad de 458 direcciones IP. ¿Cuál es la máscara de subred correcta para lograr esta división, manteniendo el número de subredes en su máximo posible? Escriba el valor correcto:

Respuesta:
255.255.254.0

Página: 71

186. Usted se encuentra configurando una subred en la oficina de la sucursal que la empresa posee en Madrid. Necesita asignar una dirección IP a los nodos en esa subred. Se le ha indicado utilizar la máscara de subred 255.255.255.224. ¿Qué direcciones IP de las siguientes serán direcciones válidas? (elija 3)

A. 15.234.118.63
B. 92.11.178.93
C. 134.178.18.56
D. 192.168.16.87
E. 201.45.116.159
F. 217.63.12.192

Respuesta: B, C, D
Página: 71

187. ¿Cuál es el número máximo de subredes que pueden ser asignadas a una red, cuando se utiliza la dirección 172.16.0.0 y la máscara de subred 255.255.240.0?

A. 16

B. 32
C. 30
D. 14
E. La máscara de subred es inválida para esa dirección de red.

Respuesta: D
Página: 71

188. Usted ha dividido en subredes la red 213.105.72.0 utilizando una máscara de subred /28. ¿Cuántas subredes utilizables y direcciones de nodo utilizables por subred se obtienen de esta manera? (elija la más adecuada)

A. 62 redes y 2 nodos.
B. 6 redes y 30 nodos.
C. 8 redes y 32 nodos.
D. 16 redes y 16 nodos.
E. 14 redes y 14 nodos.

Respuesta: E
Página: 71

189. Está trabajando como consultor y esta planificando la instalación de una red para una gran organización. El diseño requiere de 100 subredes separadas, para lo cual se ha obtenido una dirección clase B.

¿Qué máscara de subred la permitirá armar las 100 subredes requeridas, si se requieren 500 nodos utilizables por subred?

A. 255.255.240.0
B. 255.255.248.0
C. 255.255.252.0
D. 255.255.254.0
E. 255.255.255.0
F. 255.255.255.192

Respuesta: D
Página: 71

190. ¿Cuál es la dirección de red para un nodo con la dirección IP 123.200.8.68/28?

A. 123.200.8.0

D. 123.200.8.65
E. 123.200.8.31
F. 123.200.8.1

Respuesta: C
Página: 71

191. ¿Qué comando de edición desplaza su cursor hacia atrás una palabra?

A. `Ctrl+E`
B. `Ctrl+F`
C. `Esc+B`
D. `Ctrl+A`

Respuesta: C
Página: 128

192. Ha dividido la red 201.105.13.0 utilizando una máscara de subred de 26 bits. ¿Cuántas subredes utilizables y cuántas direcciones de noto utilizables por subred dispondrá de esta manera?

A. 64 redes y 4 nodos.
B. 4 redes y 64 nodos.
C. 4 redes y 62 nodos.
D. 62 redes y 2 nodos.

Respuesta: C
Página: 71

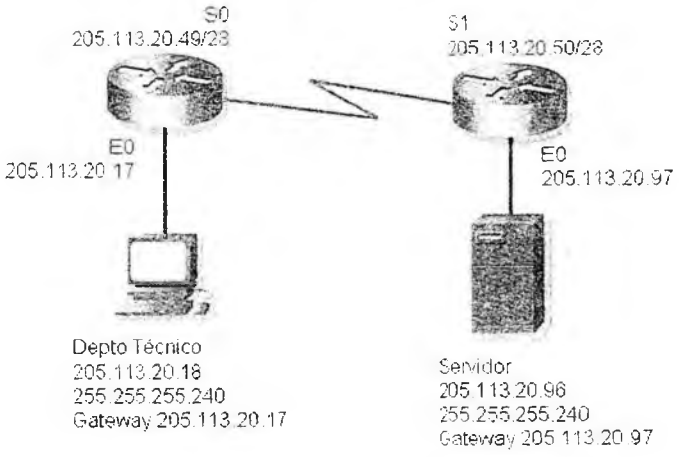
193. De los que se enumeran a continuación, ¿qué dispositivo opera en las siete capas del modelo OSI? (elija 3).

A. Terminal
B. Terminal de administración de red
C. Transceiver
D. Puente
E. Web Server
F. Switch

Respuesta: A, B, E
Página: 20, 21

194. Los clientes pertenecientes al Departamento Técnico reportan problemas de acceso. No tienen posibilidad de conectarse con el nuevo servidor de una sucursal remota.

¿Cuál es posiblemente la causa del problema?



A. El default gateway de las estaciones de trabajo del Departamento Técnico es incorrecto.
B. La máscara de subred de las estaciones de trabajo en el Departamento Técnico es incorrecta.
C. El default gateway del servidor de la Sucursal es incorrecto.
D. La dirección IP del nuevo servidor es inválida.
E. La interfaz Serial 0 del router Central y la interfaz Serial 1 del router Sucursal no se encuentran en la misma subred.

Respuesta: D
Página: 71

195. Teniendo en cuenta los siguientes criterios para permitir el acceso desde sitios remotos a su LAN:

- Restringir el acceso en la interfaz Ethernet 1.
- Ethernet 1 = 207.87.81.173.
- Denegar el acceso a telnet, ftp, snmp.
- Permitir todo tipo de operaciones.

¿Cuál de las siguientes debiera ser la última sentencia en ingresar en su lista de acceso?

A. `access-list 101`
B. `access-list 101 deny e0 telnet ftp`
C. `access-list 101 allow all except ftp telnet`
D. `access-list 101 permit ip 0.0.0.0 255.255.255.255 any`

E. `access-list 101 deny ip 207.87.81.173 tcp eq 20 21 23`

Respuesta: D
Página: 193

196. Usted tiene un enlace serial directo a un router adyacente. No tiene conectividad, y cuando ejecuta show running-config, la consola le informa que la interfaz serial está shutdown. Ahora ejecuta show interfaces serial0

¿Qué información debería encontrar reflejada en la consola?

A. serial 0 is up, line protocol is down
B. serial 0 is down, line protocol is down
C. serial 0 is down, line protocol is up
D. serial 0 is administratively down, line protocol is down
E. serial 0 is administratively down, line protocol is up
F. serial 0 is administratively up, line protocol is down

Respuesta: D
Página: 255, 256

197. Se ha comenzado a diseñar una nueva red para su empresa. Utilizando una red IP clase C, ¿qué máscara de subred la provee de 1 subred utilizable para cada departamento a la vez que permite suficiente cantidad de direcciones de nodo para cada departamento especificado en la siguiente tabla?

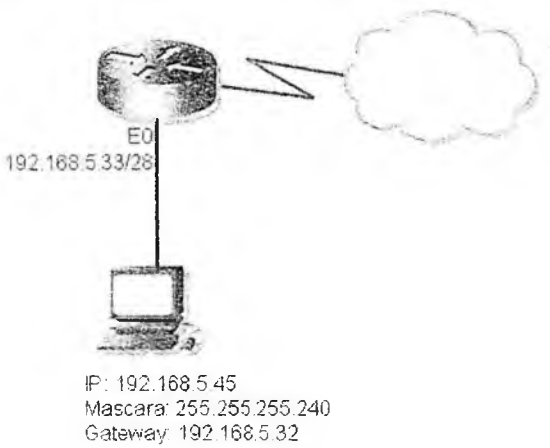
Gerencia	17 usuarios
Soporte	15 usuarios
Finanzas	13 usuarios
Ventas	07 usuarios
Desarrollo	16 usuarios

A. 255.255.255.0
B. 255.255.255.192

E. 255.255.255.248
F. 255.255.255.252

Respuesta: C
Página: 71

198. Como administrador se le ha solicitado que repare la red que se muestra más abajo. La terminal de trabajo está conectada a la red pero no logra conectarse a los recursos disponibles en otras redes a través de una nube RDSI. Asumiendo que la LAN está configurada de la siguiente manera:



¿Cuál de las siguientes es la causa de este problema?

A. El default gateway es una dirección de subred.
B. El default gateway está en una subred diferente que la terminal.
C. La máscara de subred de la terminal no coincide con la máscara de subred de la interfaz del router a la que está conectada.
D. La dirección IP de la terminal está en una subred diferente que el default gateway.

Respuesta: A
Página: 71

199. En un contexto Frame-Relay, ¿qué identifica al PVC?

A. NCP.
B. LMI.
C. IARP.

D. DLCI.

Respuesta: D
Página: 268

200. Un administrador necesita asignar una dirección IP estática al servidor de la red. De la red 192.168.20.24/29 se ha asignado al puerto del router la primera dirección de nodo utilizable, mientras que al servidor de ventas se le debe asignar la última dirección de nodo utilizable.

¿Cuál de las siguientes opciones muestra la información que se debe introducir en la caja de propiedades IP del servidor de ventas?

A.
```
Dirección IP 192.168.20.14
Máscara de subred 255.255.255.248
Default gateway 192.168.20.9
```

B.
```
Dirección IP 192.168.20.254
Máscara de subred 255.255.255.0
Default gateway 192.168.20.1
```

C.
```
Dirección IP 192.168.20.30
Máscara de subred 255.255.255.248
Default gateway 192.168.20.25
```

D.
```
Dirección IP 192.168.20.30
Máscara de subred 255.255.255.240
Default gateway 192.168.20.17
```

E.
```
Dirección IP 192.168.20.30
Máscara de subred 255.255.255.240
Default gateway 192.168.20.25
```

Respuesta: C
Página: 71

201. Se le ha sido asignada una dirección de red clase C. Su director le ha solicitado crear 30 subredes con al menos 5 nodos por subred para los diferentes departamentos en su organización. ¿Cuál es la máscara de subred que le permitirá crear esas 30 subredes?

Respuesta:
255.255.255.248

Página: 71

202. Dada la dirección IP 195.106.14.0/24, ¿cuál es el número total de redes y el número total de nodos por red que se obtiene?

A. 1 red con 254 nodos.
B. 2 redes con 128 nodos.
C. 4 redes con 64 nodos.
D. 6 redes con 30 nodos.

Respuesta: A
Página: 71

203. ¿Qué comando le mostrará la versión del IOS actualmente en ejecución en su router?

A. `show flash`
B. `show flash file`
C. `show ip flash`
D. `show version`

Respuesta: D
Página: 129, 130

204. Partiendo de la red 192.141.27.0/28, identifique las direcciones de nodo válidas (elija 3).

A. 192.141.27.33
B. 192.141.27.112
C. 192.141.27.119
D. 192.141.27.126
E. 192.141.27.175
F. 192.141.27.208

Respuesta: A, C, D
Página: 71

205. Su compañía utiliza una dirección de red clase C. Necesita crear 5 subredes con al menos 18 nodos por subred.

¿Cuál debe ser la máscara de subred para esta red?

Respuesta:
255.255.255.224

Página: 71

206. Utilizando la dirección 192.64.10.0/28, ¿cuántas subredes y cuántos nodos por subred están disponibles?

A. 62 subredes y 2 nodos.
B. 6 subredes y 30 nodos.
C. 8 subredes y 32 nodos.
D. 16 subredes y 16 nodos.
E. 14 subredes y 14 nodos.

Respuesta: E
Página: 71

207. ¿Cuál es una dirección de difusión perteneciente a la red 192.57.78.0/27?

A. 192.157.78.33
B. 192.57.78.64
C. 192.57.78.87
D. 192.57.78.97
E. 192.57.78.159
F. 192.57.78.254

Respuesta: E
Página: 71

208. ¿Cuál es el tipo de LMI por defecto?

A. q.933a
B. ansi
C. ietf
D. cisco

Respuesta: D
Página: 270

209. ¿Cuál es el patrón de bits para el primer octeto de una dirección de red clase B como 129.107.0.0?

A. 0xxxxxxx

B. 10xxxxxx
C. 110xxxxx
D. 1110xxxx
E. 11110xxx

Respuesta: B
Página: 68

210. Se está configurando una impresora de red. Desea utilizar la última dirección IP de su subred para esa impresora. Ha ejecutado un ipconfig en su terminal de trabajo y ha recibido la información que tiene más arriba. Basándose en la dirección IP y la máscara de subred de su terminal de trabajo, ¿cuál es la última dirección IP disponible en su subred?

```
Dirección IP: 172.20.7.160
Máscara de subred: 255.255.255.192
```

A. 172.20.7.255
B. 172.20.7.197
C. 172.20.7.190
D. 172.20.7.129
E. 172.20.255.255

Respuesta: C
Página: 71

211. Asumiendo que nuestra red esta utilizando una versión antigua de UNIX, ¿cuál es el número máximo de subredes que pueden ser asignadas a la red cuando utiliza la dirección 131.107.0.0 con una máscara de subred de 255.255.240.0?

A. 16.
B. 32.
C. 30.
D. 14.
E. Es una máscara de subred inválida para esta red.

Respuesta: D
Página: 71

212. ¿Cuáles son las dos formas en las que se puede entrar al modo setup en un router?

A. Tecleando el comando clear flash.
B. Tecleando el comando erase startup-config y reiniciando el router.
C. Utilizando el comando setup.

D. Tecleando el comando setup mode.

Respuesta: B, C
Página: 109

213. Si quisiera hallar todos los comandos que comenzaran con "cl" a partir de un determinado prompt, ¿qué tipearía en dicho prompt en particular?

A. `Show commands cl`
B. `cl ?`
C. `cl?`
D. `cl ? more`

Respuesta: C
Página: 110

214. Si está en modo privilegiado y quiere regresar al modo usuario, ¿qué comando deberá utilizar?

A. `exit`
B. `quit`
C. `disable`
D. `Control+Z`

Respuesta: C
Página: 110

215. ¿Qué comando de edición desplaza su cursor hasta el principio de la línea?

A. `Ctrl+E`
B. `Ctrl+F`
C. `Ctrl+B`
D. `Ctrl+A`

Respuesta: D
Página: 128

216. Se encuentra trabajando en las siguientes redes:

172.16.32.0/20
172.16.64.0/20
172.16.82.90/20

¿Cuál de las direcciones que se muestran a continuación es una dirección de difusión de las subredes de nuestra red?

A. 172.16.32.255
B. 172.16.47.255
C. 172.16.34.255
D. 172.16.82.255
E. 172.16.79.255
F. 172.16.95.255

Respuesta: B, E, F
Página: 71

217. ¿Qué comando le mostrará los contenidos de la EEPROM en su router?

A. `show flash`
B. `show flash file`
C. `show ip flash`
D. `show version`

Respuesta: A
Página: 121

218. ¿Qué comando le mostrará si el cable que se encuentra conectado a la interfaz serial 0 es DTE o DCE?

A. `show interfaces serial0`
B. `show interfaces serial 0`
C. `show controllers serial 0`
D. `show controllers serial0`

Respuesta: C
Página: 256

219. ¿Qué comando impedirá que los mensajes del sistema operativo, que por defecto están dirigidos a la consola, se escriban sobre el comando que está intentando ingresar en el prompt?

A. `no logging`
B. `logging`
C. `logging asynchronous`
D. `logging synchronous`

Respuesta: D
Página: 113

220. ¿Qué comando permitirá a los usuarios conectarse por telnet a un router sin que aparezca el prompt pidiéndoles una contraseña del modo usuario?

A. `login`
B. `no login`
C. Se puede hacer telnet por defecto, de modo tal que no se necesita un comando.
D. `no password`

Respuesta: B
Página: 114

221. Existe algún problema sobre la seguridad de su red. Posee un router que está conectado a Internet y no desea que publique actualizaciones RIP a través de la interfaz que está conectada a Internet. ¿Qué comando le permite prevenir que estas actualizaciones salgan a través de la interfaz, sin recurrir al uso de listas de acceso?

A. `passive route`
B. `default routes`
C. `passive-interface`
D. `route update filtering`

Respuesta: C
Página: 152

222. ¿Cómo configura su línea de terminal virtual 1 solamente con la contraseña "pepe"?

A.
```
line vty 0 1
login
password pepe
```
B.
```
line vty 0 4
login
password pepe
```
C.
```
Line vty 1
login
password pepe
```
D.
```
line vty 1
password pepe
login
```

Respuesta: C
Página: 113

223. ¿Cuál de las siguientes opciones es verdadera acerca de las enable passwords? (elija todas las que se apliquen).

A. La enable password se encripta por defecto.
B. La enable secret se encripta por defecto.
C. La password enable-encriptada debe configurarse primero.
D. La enable password está por encima de la enable secret.
E. La enable secret está por encima de la enable password.
F. La password enable-encriptada está por encima de todas las otras passwords.

Respuesta: B, E
Página: 112

224. ¿Qué comando configurará su consola para que se desconecte automáticamente por tiempo vencido después de solo un segundo?

A. `timeout 1 0`
B. `timeout 0 1`
C. `exec-timeout 1 0`
D. `exec-timeout 0 1`

Respuesta: D
Página: 113

225. ¿Qué comando le mostrará el nombre de nodo resuelto a la dirección IP en un router?

A. `show router`
B. `show hosts`
C. `show ip hosts`
D. `show name resolution`

Respuesta: B
Página: 123

226. ¿Cómo se entra desde el modo de configuración para poder configurar la contraseña del puerto auxiliar?

A. `line aux 1`
B. `line aux 0`
C. `line aux 0 4`
D. `line aux port`

Respuesta: B
Página: 114

227. ¿Qué comando se debe introducir para efectuar una copia de seguridad de la configuración que se ejecuta actualmente (configuración activa) y hacer que se vuelva a cargar si el router es reiniciado?

A. `Router(config)#copy current to starting`
B. `Router#copy starting to running`
C. `Router(config)#copy running-config startup-config`
D. `Router#copy running-config startup-config`

Respuesta: D
Página: 124

228. Al utilizar el modo setup, ¿cuáles son las dos opciones de configuración diferentes que ofrece este modo?

A. Básica.
B. Avanzada.
C. Extendida.
D. Expandida.

Respuesta: A, C
Página: 109

229. ¿En qué modos de un router Cisco se puede utilizar el ping de ICMP para diagnosticar una red? (elija 2).

A. Usuario.
B. Privilegiado.
C. Configuración global.
D. Configuración de la interfaz.

Respuesta: A, B
Página: 141

230. ¿Qué comando borra los contenidos de la NVRAM en un router?

A. `delete NVRAM`
B. `delete startup-config`
C. `erase NVRAM`
D. `erase startup-config`

Respuesta: D
Página: 126

231. ¿Qué comando le muestra todos los protocolos enrutados y las interfaces en las cuales cada protocolo se encuentra habilitado?

A. `show protocols`
B. `show protocol brief`
C. `show interfaces protocol`
D. `show interfaces`
E. `show routed`
F. `show routed interfaces`

Respuesta: A
Página: 167

232. ¿Cuál de las secuencias de comandos que se enuncian a continuación permite configurar una subinterfaz en su interfaz FastEthernet?

A.
```
configure terminal
interface Fastethernet 0.24010
```
B.
```
configure terminal
interface Fastethernet 100.0
```
C.
```
configure terminal
24000 Fastethernet 0
```
D.
```
configure terminal
24000 Fastethernet 100
```

Respuesta: A
Página: 244

233. ¿Cuál es el problema de una interfaz si usted ejecuta el comando show interfaces serial 0 y recibe el siguiente mensaje?

```
Serial0 is administratively down,line protocol is down
```

A. Los temporizadores de actividad son diferentes.
B. El administrador tiene deshabilitada la interfaz.
C. El administrador está haciendo ping desde la interfaz.
D. No hay ningún cable conectado.

Respuesta: B
Página: 120

234. ¿Qué comando permite ver la configuración del registro de configuración?

A. `show register`
B. `show flash`
C. `show boot`
D. `show version`

Respuesta: D
Página: 121

235. Si tipea **show interface serial 0** y recibe la siguiente respuesta,

```
RouterA#sh int s0
Serial0 is up, line protocol is down
```

¿Cuál podría ser el problema?

A. Los keepalives pueden estar mal configurados entre los enlaces punto a punto.
B. No hay un cable conectado a la interfaz.
C. El administrador necesita emitir una solicitud de no shutdown a la interfaz.
D. La interfaz es defectuosa.

Respuesta: A
Página: 257

236. Basado en la salida del comando **show interace serial0** introducido en un router **DTE**, ¿qué capa del modelo OSI es más probablemente el origen del problema?

```
Router#show interfaces serial0
Serial0 is down, line protocol is down
```

A. Capa física.
B. Capa de Datos.
C. Capa de red.
D. Capa de transporte.

Respuesta: A
Página: 119, 255

237. Para proceder a configurar una password de acceso para la consola, comienza por ejecutar el comando **Router(config)#line console 0**

¿Cuál es la operación de debiera realizar a continuación?

A. Configurar el tipo de terminal.
B. Ingresar los parámetros de protocolo para una línea serial.
C. Crear una password sobre la línea de terminal de consola.
D. Establecer una conexión terminal tipo 4 a un nodo remoto.
E. Cambiar del modo de configuración al modo privilegiado de consola.

Respuesta: C
Página: 113

238. Usted es el administrador de red de una compañía y acaba de recibir una llamada de un usuario que no puede acceder a un servidor en un sitio remoto. Después de realizar una revisión, se recoge la siguiente información:

PC local – 10.0.3.35/24
Default Gateway – 10.0.3.1
Servidor Remoto – 10.0.5.250/24

Ha realizado los siguientes tests desde la terminal que no logra el acceso:

ping 127.0.0.1 – funciona
ping 10.0.3.35 – funciona
ping 10.0.3.1 – funciona
ping 10.0.5.250 – no responde

¿A cuál de los siguientes problemas puede deberse el resultado del test realizado?

A. TCP/IP no está correctamente instalado.
B. Problemas en la capa física local.
C. La NIC de la terminal no funciona.
D. Problemas en la capa física remota.

Respuesta: D
Página: 59

239. Ha sido convocado como consultor para resolver inconvenientes en la red de una compañía. Ejecuta el comando debug ip rip a fin de diagnosticar el funcionamiento de la red RIP. Le informan que su interfaz Ethernet 10.1.0.1 ha caído.

¿Qué mensaje de actualización se visualizará en la salida del debug ip rip en su router respecto de esa red?

A. `subnet 10.1.0.0 metric 0`
B. `subnet 10.1.0.0 metric 1`
C. `subnet 10.1.0.0 metric 15`
D. `subnet 10.1.0.0 metric 16`

Respuesta: D
Página: 150

240. El ancho de banda por defecto para un enlace serial de alta velocidad es 1,544 Mbps, es decir el de una línea T1. ¿Cuál es el comando correcto para cambiar el ancho de banda de la interfaz a 64 K?

A. `bandwidth 64`
B. `band width 64`
C. `bandwidth 64000`
D. `bandwidth 64000`
E. `bandwidth 64K`

Respuesta: A
Página: 162

241. Al mirar una tabla de enrutamiento, ¿qué significa la letra "S"?
A. Conectada dinámicamente.
B. Conectada directamente.
C. Conectada estáticamente.
D. Enviando paquetes.

Respuesta: C

```
Router_A#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, * -
```

242. Router_A está directamente conectado al Router_B. En Router_A se acaba de caer la interfaz que está conectada al Router_B utilizando el comando shutdown (la ha deshabilitado administrativamente). Si introduce el comando **show interface en Router_B**, ¿qué reporte de estado de la interfaz espera ver para aquella que está conectada al Router_A?

A. `serial0 is down, line protocol is down`
B. `serial0 is administratively down, line protocol is down`
C. `serial0 is down, line protocol is up`

D. `serial0 is up, line protocol is down`
E. `serial0 is up, line protocol is up`

Respuesta: A
Página: 225

243. Router_1 no puede establecer conexión con Router_2. Utilizando el comando **show interfaces serial 0/0** en Router_1, ¿cuál es probablemente la capa del modelo OSI en la cual está el problema?

```
Router_1#show interfaces serial 0/0
Serial0/0 is down, line protocol is down
Hardware is HD64570
Internet address is 172.22.5.1/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely
255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10sec)
Last input never, output 00:03:11, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max(drops): Total output drops: 0
Queuing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max active/threshold/drops)
Conversations 0/2/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
11 packets output, 476 bytes, 0 underruns
0 output errors, 0 collisions, 27 interface resets
0 output buffer failures, 0 output buffers swapped out
11 carrier transitions
DCD=down DSR=down DTR=down RTS=down CTS=down
```

A. Capa física.
B. Capa de enlace de datos.
C. Capa de red.
D. Capa de transporte.

Respuesta: A
Página: 225

244. Se requiere configurar rápidamente 5 nuevos routers para ser chequeados. Estando conectado al router por la consola, el administrador copia y pega una configuración a partir de un archivo de texto en la ventana de HyperTerminal, parte de la cual se muestra abajo.

```
hostname Router_A
!
interface Ethernet0
ip address 192.168.10.9 255.255.255.248
!
interface Serial0
ip address 172.16.25.1 255.255.255.0
clockrate 56000
!
interface Serial1
ip address 10.1.1.1 255.255.255.0
!
router rip
network 192.168.10.0
!
line con 0
password testking
login
line aux 0
line vty 0 4
password cisco
login
!
end
```

El nodo 192.168.10.10/29 no logra ejecutar con éxito un ping a la interfaz Ethernet del router. ¿Cuál es la causa de este fallo?

A. La nueva configuración necesita ser grabada en la NVRAM antes de que los cambios tengan efecto.
B. El router necesita ser reiniciado para que los cambios se hagan efectivos.
C. La red Ethernet no es incorporada en la tabla de enrutamiento porque está incompleta la configuración de RIP.
D. La configuración que se ha copiado no sobrescribe el comando shutdown en la interfaz Ethernet.
E. La máscara de subred en el router impide que el nodo se comunique con él.

Respuesta: D
Página: 118

245. Como administrador de la red le han solicitado que permita que se establezcan sesiones telnet con un router Cisco. ¿Qué secuencia de comandos deberá utilizar?

A.
```
Router(config)#line console 0
Router(config-if)#enable password cisco
```
B.
```
Router(config)#line console 0
Router(config line)#login
Router(config-line)#enable secret cisco
```
C.
```
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password cisco
```
D.
```
Router(config)#line vty 0 4
Router(config-line)#enable password cisco
```
E.
```
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#enable secret cisco
```
F.
```
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password cisco
```

Respuesta: F
Página: 113

246. ¿Cuál es el algoritmo de enrutamiento utilizado por RIP?

A. Información enrutada.
B. Enlazar.
C. Estado del enlace.
D. Vector distancia.

Respuesta: D
Página: 150

247. ¿Cuál es el algoritmo de enrutamiento utilizado por EIGRP?

A. Información enrutada.
B. Enlazar.
C. Estado del enlace.
D. Vector de distancia.

Respuesta: D
Página: 159

248. ¿Qué comando puede ingresar en el prompt del router para verificar la frecuencia de envío de difusión para EIGRP?

A. `show ip route`
B. `show ip protocols`
C. `show ip broadcast`
D. `debug ip eigrp`

Respuesta: B
Página: 167

249. ¿Cuál es la métrica de enrutamiento por defecto utilizada por EIGRP? (elija todas las que se apliquen).

A. Cuenta al infinito.
B. Número de saltos.
C. TTL.
D. Ancho de banda.
E. Retraso.

Respuesta: D, E
Página: 161

250. ¿Para qué se utilizan los temporizadores de espera?

A. Para impedir momentáneamente que el protocolo se dirija al siguiente salto.
B. Para evitar que los mensajes de actualización regulares vuelvan a anunciar que una ruta está inactiva.
C. Para evitar que los mensajes de actualización regulares vuelvan a anunciar que una ruta acaba de activarse.
D. Para evitar que los mensajes de actualización irregular vuelvan a anunciar que una ruta está inactiva.

Respuesta: B
Página: 97

251. Respecto a Frame-Relay, ¿cuál de las siguientes afirmaciones es verdadera?

A. Debe utilizarse encapsulación Cisco si se conecta a un equipamiento no Cisco.
B. Debe utilizarse encapsulación ANSI si se conecta a un equipamiento no Cisco.
C. Debe utilizarse encapsulación IETF si se conecta a un equipamiento no Cisco.
D. Debe utilizarse encapsulación Q.933A si se conecta a un equipamiento no Cisco.

Respuesta: B
Página: 270

252. ¿Cuál es la distancia administrativa por defecto para EIGRP?

A. 90
B. 100
C. 120
D. 220

Respuesta: A
Página: 91

253. ¿Cuál de las siguientes afirmaciones es verdadera respecto de la regla de horizonte dividido?

A. Solamente un router puede dividir la frontera (horizonte) entre redes concéntricas.
B. Todos los protocolos de vector distancia requieren enviar hacia atrás las rutas que pueden causar momentáneamente bucles ante el cambio de topología.
C. Las redes solo pueden mantener convergencia completa si toda la información referida a rutas es enviada a través de todas las interfaces activas.
D. La información referida a una ruta no puede ser enviada nuevamente en la misma dirección desde la cual se recibió la información original.
E. Cada sistema autónomo mantiene tablas de enrutamiento convergentes para prevenir el descarte de rutas debido a actualizaciones que se reciben desde fuera de los límites (horizonte) del sistema autónomo.

Respuesta: D
Página: 96

254. ¿Cuál de las siguientes opciones es una ruta por defecto correcta?

A. `route ip 172.0.0.0 255.0.0.0 serial 0/0`
B. `ip route 0.0.0.0 0.0.0.0 172.16.20.1`
C. `ip route 0.0.0.0 255.255.255.255 172.16.20.1`
D. `route ip 0.0.0.0 0.0.0.0 172.16.10.1150`

Respuesta: B
Página: 90

255. ¿Qué comandos están disponibles para soportar redes RIP? (elija 2).

A. `show ip route`
B. `show ip rip`
C. `show rip network`
D. `debug ip rip`

Respuesta: A, D
Página: 155

256. ¿Qué comando Cisco IOS puede utilizar para ver la tabla de enrutamiento IP?

A. `show ip config`
B. `show ip arp`
C. `show ip route`
D. `show ip table`

Respuesta: C
Página: 39, 154

257. Un técnico se encuentra configurando un router denominado Router_2. ¿Para qué utilizaría el comando passive-interface?

A. Permitir a los protocolos de enrutamiento enviar actualizaciones a través de una interfaz que no tiene dirección IP.
B. Permitir a un router enviar actualizaciones de enrutamiento a través de una interfaz pero no recibir actualizaciones a través de esa interfaz.
C. Permitir a una interfaz permanecer activa aunque no reciba keepalives.
D. Permitir que un grupo de interfaces compartan una misma dirección IP.
E. Permitir a un router recibir actualizaciones de enrutamiento a través de una interfaz pero no enviar actualizaciones a través de esa misma interfaz.

Respuesta: E
Página: 152, 164

258. ¿Cuál de las siguientes opciones es verdadera respecto del procedimiento para crear rutas estáticas? (elija 2).

A. El parámetro de la máscara es opcional.
B. Se requiere el parámetro del gateway.
C. Se requiere la distancia administrativa.
D. La distancia administrativa es opcional.
E. Ninguna de las opciones anteriores.

Respuesta: B, D
Página: 89

259. ¿Cuál de las siguientes opciones es verdadera acerca del enrutamiento IP?

A. La dirección IP de destino cambia en cada salto.
B. La dirección IP de origen cambia en cada salto.
C. La trama no cambia en cada salto.
D. La trama cambia en cada salto.

Respuesta: C
Página: 100

260. ¿Cuál de los siguientes elementos encontrará en una tabla de enrutamiento? (elija todas las que se apliquen).

A. Dirección de red destino.
B. Métrica de enrutamiento.
C. Interfaz de salida para paquetes.
D. Interfaz de entrada.

Respuesta: A, B, C
Página: 88

261. ¿Cuál es la distancia administrativa por defecto de RIP?

A. 1
B. 100
C. 120
D. 150

Respuesta: C
Página: 91

262. ¿Qué significa una distancia administrativa de 0?

A. 0 es la distancia administrativa por defecto para el enrutamiento dinámico.
B. 0 es la distancia administrativa por defecto para las rutas directamente conectadas.
C. No hay un enrutamiento permitido en este router.
D. Hay 0 saltos al siguiente destino.

Respuesta: B
Página: 91

263. ¿Cómo se crea una ruta por defecto?

A. Utilizando 1 en el lugar de la red y la máscara.
B. Definiendo una ruta estática y utilizando 0 en el lugar de la red y la máscara.
C. Utilizando 255 en el lugar de la red y la máscara.
D. Login [nombre, contraseña].

Respuesta: B
Página: 90, 148

264. ¿Qué parámetro debe ser suministrado cuando se inicializa el proceso de enrutamiento con EIGRP?

A. Número de redes conectadas.
B. Máscara de direccionamiento IP.
C. Peso de las métricas.
D. Número de sistema autónomo.
E. ID administrativo registrado.

Respuesta: D
Página: 162

265. Una tabla de enrutamiento contiene rutas estáticas y rutas aprendidas por RIP y EIGRP para la misma red de destino. ¿Qué ruta será normalmente utilizada para reenviar los datos?

A. La ruta de EIGRP.
B. La ruta estática.
C. La ruta de RIP.
D. Hará balanceo de tráfico entre las 3 rutas.

Respuesta: B
Página: 145, 147

266. Se encuentra configurando una red en la oficina central de una empresa en Burgos, para lo que utiliza protocolos de vector distancia.

¿Qué herramientas se implementan para prevenir bucles de enrutamiento en la red?

A. Avisos de estado de enlace (LSA).
B. Protocolo de árbol de expansión.
C. Árbol de primero la ruta más corta.
D. Horizonte dividido.
E. Temporizadores de espera.

Respuesta: D, E
Página: 96

267. Está observando una tabla de enrutamiento IP en un router Cisco. ¿Qué enunciados de los siguientes describen correctamente los códigos utilizados en la tabla de enrutamiento? (elija 2).

A. I – Indica una ruta aprendida a través de un protocolo interno.
B. S – Indica una ruta ingresada manualmente.
C. R – Indica una ruta aprendida a través de RIP.
D. S – Indica una ruta aprendida a través de un puerto serie.
E. C – Indica una ruta aprendida a través de un puerto confiable.

Respuesta: B, C
Página: 154

```
Router_A#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, * -
```

268. Si RIP utiliza la cuenta de saltos para determinar la mejor ruta, ¿qué es lo que utiliza EIGRP?

A. El mayor valor de métrica.
B. El menor valor de una métrica compuesta.
C. La menor cuenta de saltos y retraso.
D. El mayor ancho de banda y confiabilidad.
E. La menor distancia administrativa.

Respuesta: B
Página: 161

269. Para poder realizar el enrutamiento de modo adecuado y eficiente, ¿qué debe tener un router?

A. Aplicación de destino del paquete que está recibiendo.
B. Número de otros paquetes que componen un mismo flujo de datos.
C. Dirección de red de destino del paquete que está recibiendo.
D. Número de routers que conocen una ruta hasta el destino.

Respuesta: C
Página: 88

270. Se necesita ingresar el comando **show startup-config** desde el modo privilegiado. ¿Que símbolo le indica que se encuentra en el modo privilegiado?

A. >
B. !
C. #
D. :

Respuesta: C
Página: 109, 125

271. ¿Qué comando copiará la imagen del IOS almacenada en la memoria flash de su router a un servidor TFTP de respaldo de su red?

A. `transfer IOS to 172.16.10.1`
B. `copy running-config startup-config`
C. `copy tftp flash`
D. `copy startup-config tftp`
E. `copy flash tftp`

Respuesta: E
Página: 126

272. El administrador de la red ha encontrado el siguiente problema. Las redes remotas 172.16.10.0, 172.16.20.0 y 172.16.30.0 son accesibles a través de la interfaz serial 0 del Router_A. Los usuarios no pueden acceder a 172.16.20.0. Después de revisar el resultado de los siguientes comandos,

```
Router_A#debug ip rip
.....
ld00h: RIP:received v1 update from 172.16.100.2 on Serial 0/0
ld00h: 172.16.10.0 in 1 hops
ld00h: 172.16.20.0 in 1 hops
ld00h: 172.16.30.0 in 1 hops
```

```
Router_A#show ip route
Gateway of last resort is not set
172.16.0.0/24 is subnetted, 8 subnets
C 172.16.150.0 is directly connected, FastEthernet 0/0
C 172.16.220.0 is directly connected, Loopback2
C 172.16.210.0 is directly connected, Loopback1
C 172.16.200.0 is directly connected, Loopback0
R 172.16.30.0 [120/1] via 172.16.100.2, 00:00:07, Serial 0/0
S 172.16.20.0 [1/0] via 172.16.150.15
R 172.16.10.0 [120/1] via 172.16.100.2, 00:00:07, Serial 0/0
C 172.16.100.0 is directly connected, Serial 0/0
```

¿cuál es más probablemente la causa del problema?

A. No hay configurada una ruta por defecto en Router_A.
B. El Router_A no está recibiendo actualizaciones de la red 172.16.20.0.
C. Es incorrecta la ruta estática para 172.16.20.0.
D. 172.16.20.0 no se encuentra en la tabla de enrutamiento de Router_A.

Respuesta: C

La recepción de las actualizaciones de RIP llegan por la interfaz Serial0/0 desde 172.16.100.2, es decir el próximo salto. La ruta estática debería apuntar hacia dirección IP pero no lo hace:

```
S 172.16.20.0 [1/0] via 172.16.150.15
```

273. ¿Qué comando mostrará las interfaces habilitadas para trabajar con CDP en un router?

A. `show cdp`
B. `show cdp interfaces`
C. `show interfaces`
D. `show cdp traffic`

Respuesta: B
Página: 137

274. ¿Cuáles son los temporizadores de actualización y tiempo de espera por defecto para CDP?

A. 240, 90
B. 90, 240
C. 180, 60
D. 60, 180

Respuesta: D
Página: 136

275. Como administrador de la red se encuentra configurando listas de acceso sobre una interfaz de un router Cisco. Utiliza múltiples listas de acceso. ¿Cuál de las siguientes afirmaciones es válida?

A. No hay límite para el número de listas de acceso que pueden ser aplicadas a una interfaz, con la condición de que sean aplicadas desde las más específicas a las más generales.
B. Cisco IOS permite aplicar solamente una lista de acceso a una interfaz.
C. Una lista de acceso puede ser configurada por dirección para cada protocolo de capa configurado en una interfaz.
D. Hasta 3 listas de acceso por protocolo pueden ser aplicadas a una interfaz individual.
E. No más de 2 listas de acceso pueden ser aplicadas sobre una interfaz individual.
F. El número máximo permitido varía dependiendo de la cantidad de RAM instalada en el router.

Respuesta: C
Página: 214

276. Basados en la información del comando show ip route, ¿qué ruta de las siguientes no será ingresada en el router vecino que utiliza RIP?

```
Router_A#show ip route
Codes: C-connected,s-static,I-IGRP,R-RIP,M-Mobile,B-BGP
D-EIGRP,EIGRP external, O-OSPF,IA-OSPF inter area,
EI-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

Gateway of last resort is not set

R 192.168.8.0/24 [120/1] via 192.168.2.2, 00:00:10, Serial0
C 192.168.9.0/24 is directly connected, Serial 1
R 192.168.10.0/24 [120/7] via 192.168.9.1, 00:00:02, Serial1
R 192.168.11.0/24 [120/7] via 192.168.9.1, 00:00:03, Serial1
C 192.168.1.0/24 is directly connected, Ethernet0
C 192.168.2.0/24 is directly connected, Serial0
R 192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:10, Serial0
R 192.168.4.0/24 [120/15] via 192.168.2.2, 00:00:10, Serial0
R 192.168.5.0/24 [120/15] via 192.168.2.2, 00:00:10, Serial0
R 192.168.6.0/24 [120/15] via 192.168.2.2, 00:00:10, Serial0
R 192.168.7.0/24 [120/1] via 192.168.2.2, 00:00:10, Serial0
```

A. `R 192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:10, Serial0`

B. `R 192.168.11.0/24 [120/7] via 192.168.9.1, 00:00:03, Serial1`

C. `C 192.168.1.0/24 is directly connected, Ethernet0`

D. `R 192.168.5.0/24 [120/15] via 192.168.2.2, 00:00:10, Serial0`

Respuesta: D
Página: 154

Los dos valores dentro de los corchetes indican la distancia administrativa y la métrica, que en este caso ha llegado al límite 15, el próximo salto será inalcanzable.

277. La red 131.107.4.0/24 ha sido publicada por un router vecino utilizando RIP y EIGRP, también ha agregado una ruta estática a 131.107.4.0/24 manualmente. ¿Cuál ruta será utilizada para reenviar tráfico?

A. La ruta EIGRP.
B. La ruta estática.
C. La ruta RIP.
D. Balanceará tráfico entre las 3 rutas.

Respuesta: D

El router recibe información desde dos protocolos diferentes, sumado a la configuración de una ruta estática en el propio dispositivo, lo que significa que el router conoce la ruta hacia el destino de tres formas diferentes balanceando la carga por ellas.

278. Para configurar el Router_A para que trabaje en un entorno Frame-Relay, uno de los items que se recomienda que se configure es la métrica para la velocidad de los enlaces EIGRP. ¿Qué comando se debe utilizar para esto?

A. `Router_A(config-if)#eigrp metric 36k`
B. `Router_A(config)#bandwidth 36`
C. `Router_A(config)#metric 36k`
D. `Router_A(config-if)#bandwidth 36`
E. `Router_A(config-if)#bandwidth 36000`

Respuesta: D
Página: 162, 271

279. ¿Cuál de las siguientes es un ejemplo de una dirección MAC de capa 2?

A. 192.201.63.251
B. 19-22-01-63-25

C. 0000.1234.FEG
D. 00-00-12-34-FE-AA

Respuesta: D
Página: 32

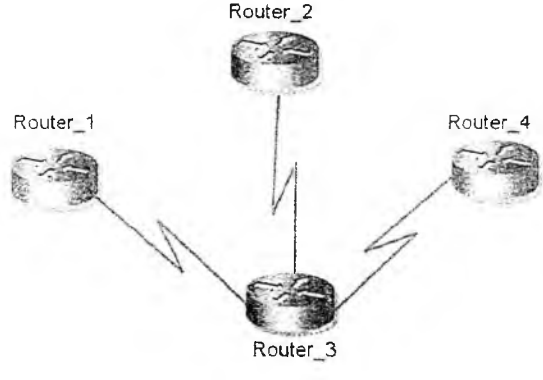
280. Basados en la salida del comando que se muestra más abajo, ¿qué representa [120/3]?

```
Router_A#show ip route
<some output text omitted>
Gateway of last resort is not set.
I 172.16.0.0[110/84632] via 192.168.6.3,00:00:13,
FastEthernet0/0
R 192.168.3.0[120/3] via 192.168.2.2,00:00:09, Serial0/0
C 192.168.2.0 is directly connected, Serial 0/0
C 192.168.6.0 is directly connected, FastEthernet0/0
```

A. 120 es el puerto UDP para reenviar tráfico y 3 es el número de saltos.
B. 120 es la distancia administrativa y 3 es la métrica para esa ruta.
C. 120 es el ancho de banda del enlace y 3 es el número de proceso de enrutamiento.
D. 120 es el valor del temporizador de actualización y 3 es el número de actualizaciones recibidas de esa ruta.

Respuesta: B
Página: 154

281. Teniendo en cuenta la siguiente topología, y asumiendo que todos los routers están ejecutando RIP, ¿qué afirmación de las siguientes describe cómo los routers intercambian sus tablas de enrutamiento? (elija 2)



A. Router_1 intercambia con Router_3.
B. Router_1 intercambia con Router_4.
C. Router_1 intercambia con Router_2.
D. Router_4 intercambia con Router_3.
E. Router_4 intercambia con Router_1.
F. Router_4 intercambia con Router_2.

Respuesta:

Se intercambia información directamente desde el vecino correspondiente.

282. ¿Cuál de los siguientes protocolos utiliza características tanto de los protocolos de vector distancia como de los de estado de enlace?

A. RIP.
B. OSPF.
C. EIGRP.
D. IGRP.

Respuesta: C
Página: 160

283. Se ha decidido remover el enrutamiento por RIP de los routers e instalar EIGRP. Ya se ha ejecutado el comando no **router rip** en todos los routers. Ahora es preciso instalar EIGRP. ¿Cuáles son lo comandos que se deberán utilizar para habilitar el enrutamiento por EIGRP?

A.
```
router eigrp 100
network 192.168.1.0
network 10.0.0.0
```

B.
```
router eigrp 100
network 192.168.1.0
network 10.2.0.0
```

C.
```
router eigrp 100
network 192.168.1.0 192.168.1.1
network 10.2.0.0 10.2.1.1
```

D.
```
router eigrp 100
network 192.168.1.0 255.255.255.0
network 10.2.0.0 255.255.0.0
```

Respuesta: A
Página: 162

284. ¿Qué función propia de la capa de transporte permite impedir que se sobrecargue el buffer de una terminal?

A. Segmentación.
B. Paquetes.
C. Confirmaciones de recepción.
D. Control de flujo.
E. PDU.

Respuesta: D
Página: 42

285. Su gerente de tecnología le ha comentado que desea considerar un cambio en los protocolos de enrutamiento implementados en la red, para lo que le ha solicitado le señale tres características propias de los protocolos de estado de enlace.

A. Los paquetes se enrutan sobre la base de la ruta más corta hacia el destino.
B. Las rutas son seleccionadas tomando como criterio base el factor de coste de contratación de los enlaces.
C. El intercambio de actualizaciones se dispara a partir de cambios en la red.
D. En una red multipunto, todos los routers intercambian las tablas de enrutamiento directamente con todos los otros routers.
E. Todo router en un área OSPF es capaz de representar la topología íntegra de la red.
F. Solamente el router designado en un área OSPF es capaz de representar la topología íntegra de la red.

Respuesta: A, C, E
Página: 97

286. ¿Qué tipo de entrada en una tabla EIGRP es una ruta sucesora?

A. Una ruta de respaldo, almacenada en la tabla de enrutamiento.
B. Una ruta primaria, almacenada en la tabla de enrutamiento.
C. Una ruta de respaldo, almacenada en la tabla topológica.
D. Una ruta primaria, almacenada en la tabla topológica.

Respuesta: C
Página: 160

287. ¿Sobre qué tipo de redes OSPF elige un router designado de respaldo?

A. Punto a punto y multiacceso.
B. Punto a multipunto y multiacceso.

C. Punto a punto y punto a multipunto.
D. No difusión y difusión multipunto.
E. No difusión y difusión multiacceso.

Respuesta: E
Página: 171

288. ¿Por qué es mejor utilizar un diseño jerárquico en redes OSPF? (elija 3).

A. Porque permite reducir la complejidad de la configuración del router.
B. Acelera la convergencia.
C. Confina la posible inestabilidad de la red a solo un área de la misma.
D. Reduce la sobrecarga por enrutamiento.
E. Reduce el coste de reemplazar routers.
F. Permite reducir la latencia por el incremento de ancho de banda.

Respuesta: B, C, D
Página: 51

289. ¿Cuáles de las siguientes son características del protocolo de enrutamiento EIGRP? (elija 2).

A. Tiene un número máximo de saltos de 255.
B. Utiliza una metrica de 32 bits.
C. Puede diferenciar entre rutas internas y externas.
D. Soporta un único protocolo enrutado.
E. Puede mantener solamente una tabla de enrutamiento.
F. Requiere que todas las redes en un mismo sistema autónomo utilicen la misma máscara de subred.

Respuesta: B, C
Página: 160, 163

290. María se trabaja como administradora de red y ha sido consultada sobre las diferencias entre los protocolos de vector distancia y los de estado de enlace. ¿Cuáles de las siguientes afirmaciones podrían estar en su respuesta? (elija 2)

A. Los protocolos de vector distancia envían la tabla de enrutamiento completa a los dispositivos vecinos directamente conectados.
B. Los protocolos de estado de enlace envían la tabla de enrutamiento completa a todos los routers en la red.

C. Los protocolos de vector distancia envían actualizaciones sobre los dispositivos directamente conectados a todas las redes enlistadas en la tabla de enrutamiento.
D. Los protocolos de estado de enlace envían actualizaciones conteniendo información sobre el estado de sus propios enlaces a todos los routers que se encuentran en la red.

Respuesta: A
Página: 94

291. Una interfaz OSPF ha sido configurada ingresando el comando bandwith 64. ¿Qué coste calculará OSPF para este enlace?

A. 1
B. 10
C. 1562
D. 64000
E. 128000

Respuesta: C
Página: 169

$$10^8/64000=1562,5$$

292. ¿Qué tipo de paquetes utilizan los routers que corren OSPF para mantener la conectividad con los routers vecinos?

A. Paquetes de intervalo muerto.
B. Paquetes hello.
C. Paquetes LSU.
D. Paquetes OSPF.
E. Paquetes de keepalive.

Respuesta: B
Página: 169

293. ¿Para cuál de los siguientes casos no se necesitaría disponer de un cable cruzado?

A. Conectar enlaces ascendentes entre switches.
B. Conectar routers a switches.
C. Conectar hub a hub.
D. Conectar hubs a switches.

Respuesta: B
Página: 28

294. ¿Qué información utiliza un router que corre protocolos de estado de enlace para construir y mantener su base de datos topológica? (elija 2).

A. Paquetes hello.
B. Mensajes SAP enviados por otros routers.
C. LSAs de otros routers.
D. Señales recibidas sobre enlaces punto a punto.
E. Tablas de enrutamiento recibidas desde otros routers que corren protocolos de estado de enlace.
F. Paquetes TTL de los routers designados.

Respuesta: A, C
Página: 168, 169

295. Como administrador de la red de la empresa, necesita configurar un router para que utilice OSPF y agregar la red 192.168.10.0/24 al área OSPF 0. ¿Cuál de los siguientes comandos necesitará utilizar para esto? (elija todos los que se apliquen).

A. `Router(config-router)#network 192.168.10.0 0.0.0.255 0`
B. `Router(config-router)#network 192.168.10.0 0.0.0.255 area 0`
C. `Router(config-router)#network 192.168.10.0 255.255.255.0 area 0`
D. `Router(config)#router ospf 0`
E. `Router(config)#router ospf 1`
F. `Router(config)#router ospf area 0`

Respuesta: B, E
Página: 172

296. Cuando se enruta con OSPF se utilizan áreas. ¿Cuál es la característica de estas áreas? (elija 3).

A. Las redes OSPF jerárquicas no necesitan de múltiples áreas.
B. Múltiples áreas OSPF deben ser conectadas al área 0.
C. Un área OSPF única debe ser configurada en el área 1.
D. Se puede asignar a las áreas cualquier número entre 0 y 63535.
E. El área 0 es llamada también área de backbone.
F. Cada área OSPF necesita ser configurada con una interfaz de loppback.

Respuesta: B, C, E

Página: 172, 174

297. ¿En cuál de los siguientes tipos de red OSPF no elegirá un router designado?

A. Redes punto a punto.
B. Redes de no-difusión y de difusión multipunto.
C. Redes punto a punto y de difusión multi-acceso.
D. Redes punto a multipunto y difusión multiacceso.
E. Redes de difusión y no-difusión multicacceso.

Respuesta: A
Página: 171

298. ¿Cuál de las siguientes entradas de enrutamiento EIGRP puede ser descrita como una ruta sucesora probable?

A. Una ruta primaria, almacenada en la tabla de enrutamiento.
B. Una ruta de respaldo, almacenada en la tabla de enrutamiento.
C. Una ruta de respaldo, almacenada en la tabla de topología.
D. Una ruta primaria, almacenada en la tabla de topología.

Respuesta: C
Página: 160

299. ¿Cuáles de las siguientes son características de NAT?(elija 2).

A. Dirección local interna.
B. Dirección externa local.
C. Dirección externa global.
D. Dirección local externa.

Respuesta: A, D
Página: 263

300. ¿Cuál de los diferentes tipos de paquetes mencionados más abajo es enviado entre routers que corren OSPF para mantener conectividad con los routers vecinos?

A. Paquetes OSPF.
B. Paquetes hello.
C. Paquetes de keepalive.
D. Paquetes de intervalo muerto.

Respuesta: B

Página: 169

301. Un compañero de trabajo le pregunta qué tipo de información corre en un router al utilizar un protocolo de estado de enlace para construir su base de datos topológica. ¿Qué podría decirle al respecto? (elija 2).

A. LSAs de otros routers.
B. Ráfagas recibidas sobre los enlaces punto a punto.
C. Paquetes hello.
D. Tablas de enrutamiento recibidas desde otros routers.
E. Paquetes SAP enviados por otros routers.
F. Paquetes TTL enviados por algunos routers en especial.

Respuesta: A, C
Página: 168, 169

302. Al trabajar con redes punto a punto, ¿qué dirección utilizan los paquetes hello de OSPF?

A. A. 127.0.0.1
B. B. 192.168.0.5
C. C. 223.0.0.1
D. D. 172.16.0.1
E. E. 224.0.0.5
F. F. 254.255.255.255

Respuesta: E
Página: 169

303. ¿Qué comando copiará la configuración de un router almacenada en un servidor TFTP en la NVRAM de ese router?

A. `transfer IOS to 172.16.10.1`
B. `copy running-config startup-config`
C. `copy tftp startup-config`
D. `copy tftp running-config`
E. `copy flash tftp`

Respuesta: C
Página: 124

304. Para copiar una configuración desde un servidor TFTP a la DRAM de un router Cisco en su red, ¿qué comando puede utilizar?

A. `configure memory`

B. `configure terminal`
C. `copy tftp running-config`
D. `copy tftp startup config`

Respuesta: C
Página: 124

305. Para copiar una configuración desde la DRAM de un router Cisco a un nodo TFTP de su red, ¿qué comando puede utilizar?

A. `configure network`
B. `configure memory`
C. `configure terminal`
D. `copy running-config tftp`
E. `copy startup-config tftp`

Respuesta: D
Página: 124

306. ¿Qué memoria en un router Cisco almacena los buffers de paquetes y las tablas de enrutamiento?

A. Flash.
B. RAM.
C. ROM.
D. NVRAM.

Respuesta: B
Página: 104

307. ¿Cuál de los siguientes es el comando correcto para crear una tabla que mapee nombres de nodos a direcciones IP en un router?

A. `madrid ip host 172.16.10.1`
B. `host 172.16.10.1 madrid`
C. `ip host madrid 172.16.10.1 172.16.15.1`
D. `host madrid 172.16.10.1`

Respuesta: C
Página: 123

308. ¿Qué comando le permitirá ver las conexiones efectuadas desde su router hacia un dispositivo remoto?

A. `show sessions`
B. `show users`
C. `disconnect`
D. `clear line`

Respuesta: A
Página: 142

309. ¿Cuál de los siguientes comandos le proporcionará el mismo resultado que el comando show cdp neighbors detail?

A. `show cdp`
B. `show cdp detail`
C. `show cdp neighbors`
D. `show cdp entry *`

Respuesta: D
Página: 136

310. Usted está trabajando con un antiguo router de la serie 2500. Se encuentra realizando el procedimiento de recuperación de claves y acaba de ingresar el comando **o/r 0x2142**. Un colaborador suyo que está mirando le pregunta sobre el propósito de este comando. ¿Qué podría decirle?

A. Para reiniciar el router.
B. Para saltar la configuración en la NVRAM.
C. Para visualizar la clave perdida.
D. Para guardar los cambios a la configuración.
E. Para ingresar el modo monitor de ROM.

Respuesta: B
Página: 132

311. El comando **show cdp neighbors detail**, ejecutado en un router Cisco, ¿cuál de los elementos de información que se enuncian a continuación le proporcionará? (elija 6 opciones).

A. Dirección IP del colindante.
B. Puerto/interfaz local.
C. La misma información que show version.
D. Capacidad.

E. La misma información que show cdp entry *.
F. ID del puerto remoto.
G. ID del dispositivo colindante.
H. Tiempo de espera.
I. Plataforma de hardware.
J. Velocidad del enlace.

Respuesta: B, D, F, G, H, I
Página: 136

312. ¿Qué hace el comando **cdp timer 90**?

A. Muestra la frecuencia de actualización de los paquetes CDP.
B. Cambia la frecuencia de actualización de los paquetes CDP.
C. Configura el comando de CDP colindante a 90 líneas.
D. Cambia el tiempo de espera de los paquetes CDP.

Respuesta: B
Página: 136

313. ¿Qué comando inhabilita CDP en una interfaz individual?

A. `no cdp run`
B. `no cdp enable`
C. `no cdp`
D. `disable cdp`

Respuesta: B
Página: 136

314. ¿Qué comando puede utilizar para ver qué dispositivos han efectuado telnet en su router?

A. `show vty line`
B. `show session`
C. `show users`
D. `show connections`

Respuesta: C
Página: 142

315. ¿Qué comando se utiliza para verificar la ruta que toma un paquete a través de una internetwork?

A. ping
B. trace
C. RIP
D. SAP

Respuesta: B
Página: 142

316. ¿Qué comando puede utilizar para efectuar una copia de seguridad de la configuración del router Cisco en un nodo TFTP?

A. `copy run tftp`
B. `copy flash tftp`
C. `copy nvram startup`
D. `copy tftp flash`

Respuesta: A
Página: 124

317. ¿Qué comando cancelará una conexión a un router remoto?

A. `Console>clear connection`
B. `Console>clear line`
C. `Console>disconnect`
D. `Console>clear user`

Respuesta: C
Página: 143

318. Su compañía ha adquirido algunos routers para su operación on-line. Necesita guardar una copia de respaldo del IOS y almacenarla en un servidor TFTP. ¿Cuáles de los siguientes son pasos que debe realizar antes de copiar la imagen del IOS al servidor TFTP? (elija 3).

A. Asegurarse el acceso al servidor TFTP de la red.
B. Verificar que se ha configurado la autenticación para acceder.
C. Asegurarse que el servidor tiene suficiente espacio para almacenar la imagen del IOS.
D. Verificar los requerimientos de ruta y nombre del archivo.
E. Asegurarse que el servidor puede leer y corre el código de arranque.

Respuesta: A, C, D
Página: 124

319. ¿Qué comando cancelará una conexión telnet iniciada desde una posición remota hacia su router?

A. `clear connection`
B. `clear line #`
C. `disconnect`
D. `clear user`

Respuesta: B
Página: 143

320. ¿Desde dónde leería un router la imagen del Cisco IOS si el registro de configuración se fijara en 0x0101?

A. Flash.
B. ROM.
C. Boot ROM.
D. NVRAM.

Respuesta: B
Página: 131

321. ¿Qué comando puede utilizar para copiar una nueva imagen del Cisco IOS a un router?

A. `copy tftp running-config`
B. `copy tftp flash`
C. `copy tftp startup-config`
D. `copy flash tftp`
E. `boot system flash IOS_name`

Respuesta: E
Página: 126

322. A fin de recuperar la contraseña de un router, ¿cuál de los siguientes elementos deberán ser modificados? (elija 2).

A. NVRAM.
B. Registro de configuración.
C. Boot flash.
D. CMOS.
E. Flash.

Respuesta: A, B
Página: 132

323. Se acaba de adquirir un router de la serie 2600. Por defecto, cuando el router se enciende, ¿cuál es la secuencia de búsqueda que utiliza para localizar la imagen del Cisco IOS?

A. Flash, servidor TFTP, ROM
B. NVRAM, servidor TFTP, ROM
C. ROM, Flash, servidor TFTP
D. ROM, NVRAM, servidor TFTP

Respuesta: A
Página: 108

324. Acaba de introducir el comando:

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

La IOS dispone de combinaciones de teclas que le permiten completar la sintaxis de un comando ingresado parcialmente. ¿Qué tecla o combinación de teclas deberá utilizar para completar el comando que ingresó antes de esta manera?

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

A. ctrl + shift + 6, luego x
B. ctrl + z
C. tab
D. /?
E. Shift

Respuesta: C
Página: 110, 128

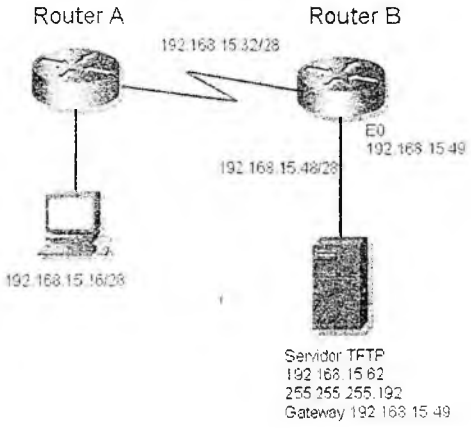
325: Full-duplex brinda la posibilidad de enviar y recibir datos al mismo tiempo. ¿Cuál de los estándares Ethernet que se mencionan a continuación puede operar en modo full-duplex?

A. 10Base2
B. 10Base5
C. 10BaseT
D. 100BaseT

Respuesta: C, D
Página: 25

326. El administrador de la red que se muestra abajo acaba de agregar el nuevo router denominado Router_B. Desea hacer una copia de respaldo de la

imagen del IOS del nuevo router en su servidor TFTP. Cuando procede a realizar la copia, el procedimiento falla. ¿Cuál puede ser la causa del problema?



A. Es incorrecto el default gateway del servidor TFTP.
B. Es incorrecta la máscara de subred del servidor TFTP.
C. Es incorrecta la dirección IP del servidor TFTP.
D. Es incorrecta la dirección IP de la interfaz E0 del Router_B.

Respuesta: B
Página: 71

327. Las características de edición avanzada de los routers están habilitadas por defecto. Para deshabilitarlas se debe introducir el comando **terminal no editing**. Teniendo activadas las características de edición avanzada, ¿cuál es el efecto de Ctrl-Z?

A. Sale para regresar al modo privilegiado.
B. Desconecta de otros routers.
C. Interrumpe una operación de ping.
D. Sale del modo privilegiado.

Respuesta: A
Página: 128

328. Su ayudante ha estado trabajando en el router mientras usted estaba ausente. ¿Qué comando le permitirá revisar cuáles son los últimos comandos que ingresó?

A. `control header`
B. `show buffer`
C. `show history`
D. `show history buffer`

Respuesta: C
Página: 112

329. ¿Qué se utiliza a nivel de la capa de enlace de datos para individualizar terminales en una red local?

A. Direcciones de red lógicas.
B. Números de puerto.
C. Direcciones de hardware.
D. Gateways por defecto.

Respuesta: C
Página: 30

330. ¿Cuál de los siguientes elementos es utilizado en las listas de acceso IP estándar como base para permitir o denegar paquetes?

A. Dirección de origen.
B. Dirección de destino.
C. Protocolo.
D. Puerto.

Respuesta: A
Página: 195

331. ¿Cuál es el rango de números que identifican una lista de acceso extendida IP?

A. 1-99
B. 20-299
C. 1000-1999
D. 100-199

Respuesta: D
Página: 201

332. ¿Qué comandos show puede utilizar para identificar el número de DLCI local? (elija 2).

A. `show frame-relay local-dlci`
B. `show frame-relay pvc`

C. `show frame-relay dlci`
D. `show frame-relay map`
E. `show ip route`

Respuesta: B, D
Página: 278

333. ¿Cuáles son los números de lista de acceso utilizados para crear listas de acceso IP estándar?

A. 1-10
B. 1-99
C. 100-199
D. 1000-1999

Respuesta: B
Página: 201

334. Para especificar todos los nodos en la red IP Clase B 172.16.0.0, ¿qué máscara de wildcard utilizaría?

A. 255.255.0.0
B. 255.255.255.0
C. 0.0.255.255
D. 0.255.255.255
E. 0.0.0.255

Respuesta: C
Página: 198

335. ¿Qué wildcard utilizaría para filtrar las redes 172.16.16.0 / 24 a 172.16.23.0 / 24?

A. 172.16.16.0 0.0.0.255
B. 172.16.255.255 255.255.0.0
C. 172.16.0.0 0.0.255.255
D. 172.16.16.0 0.0.8.255
E. 172.16.16.0 0.0.7.255
F. 172.16.16.0 0.0.15.255

Respuesta: E
Página: 198

336. ¿Cuáles de las siguientes son formas válidas de referirse solo al nodo 172.16.30.55 en una lista de acceso IP? (elija 2).

A. `172.16.30.55 0.0.0.255`
B. `172.16.30.55 0.0.0.0`
C. `any 172.16.30.55`
D. `host 172.16.30.55`
E. `0.0.0.0 172.16.30.55`
F. `ip any 172.16.30.55`

Respuesta: B, D
Página: 198

337. Después de estar revisando una serie de publicaciones de tecnología, su gerente le pregunta acerca de la utilidad de las listas de control de acceso. ¿Cuáles serían respuestas posibles? (elija 3).

A. Proteger los nodos de virus.
B. Detectar escaneo masivo de puertos.
C. Asegurar alta disponibilidad de los recursos de la red.
D. Identificar tráfico interesante para DDR.
E. Filtrar tráfico por IP.
F. Monitorizar el número de bytes y paquetes.

Respuesta: C, D, E
Página: 194

338. Existe una lista de acceso con una única consigna, ¿qué significa la palabra "any" que aparece en la consigna?

```
access-list 131 permit ip any 131.107.7.0 0.0.0.255 eq tcp
```

A. Verifica cualquiera de los bits en la dirección de origen.
B. Permite cualquier máscara de wildcard para la dirección.
C. Acepta cualquier dirección de origen.
D. Verifica cualquier bit en la dirección de destino.
E. permit 255.255.255 0.0.0.0.
F. Acepta cualquier dirección de destino.

Respuesta: C
Página: 198

339. Cisco soporta 3 tipos diferentes de LMI para Frame Relay. ¿Cuáles de los siguientes son tipos de LMI?

A. IETF.
B. Q931.
C. Q933A
D. IEEE.
E. Cisco.
F. ANSI.

Respuesta: C, E, F
Página: 270

340. ¿Cuál de los siguientes comandos es válido para crear una lista de acceso IP extendida?

A. `access-list 101 permit ip host 172.16.30.0 any eq 21`
B. `access-list 101 permit tcp host 172.16.30.0 any eq 21 log`
C. `access-list 101 permit icmp host 172.16.30.0 any ftp log`
D. `access-list 101 permit ip any eq 172.16.30.0 21 log`

Respuesta: B
Página: 202

341. ¿Qué configuración utilizando listas de acceso permite que solo el tráfico proveniente de la red 172.16.0.0 entre a la interfaz serial 0?

A.
```
access-list 10 permit 172.16.0.0 0.0.255.255
interface serial 0
ip access-list 10 in
```
B.
```
access-group 10 permit 172.16.0.0 0.0.255.255
interface serial 0
ip access-list 10 out
```
C.
```
access-list 10 permit 172.16.0.0 0.0.255.255
interface serial 0
ip access-group 10 in
```
D.
```
access-list 10 permit 172.16.0.0 0.0.255.255
interface serial 0
ip access-group 10 out
```

Respuesta: C
Página: 201

342. ¿Dónde debería colocar las listas de acceso estándar en una red?

A. En el switch más cercano.
B. Lo más cercano posible al origen.

C. Lo más cercano posible al destino.
D. En Internet.

Respuesta: C
Página: 196

343. Si aplica esta lista de acceso, ¿cuál es el efecto?

```
access.list 122 permit ip 131.107.30.0 0.0.0.255 any
```

A. Permite todos los paquetes cuyos 3 primeros octetos de la dirección de origen coinciden, a todos los destinatarios.
B. Permite todos los paquetes cuyo final de la dirección de destino coincide, y acepta todas las direcciones de origen.
C. Permite todos los paquetes que se originan en la tercera subred de la dirección de red, a todos los destinatarios.
D. Permite todos los paquetes cuyos bits de nodo de la dirección de origen coinciden, a todos los destinatarios.
E. Permite todos los paquetes cuyos 3 primeros octetos de la dirección de destino coinciden

Respuesta: A
Página: 202

344. Su jefe está preocupado respecto de la seguridad de la subred 10.0.1.0/24 que contiene al servidor de contaduría. Desea estar seguro de que los usuarios no podrán conectarse utilizando telnet a ese servidor, y le ha consultado en orden a incorporar una sentencia a la lista de acceso existente para prevenir que los usuarios puedan acceder al servidor vía telnet.

¿Cuál de las siguientes sentencias debería agregar?

A. `access-list 15 deny tcp 10.0.1.0 255.255.255.0 eq telnet`
B. `access-list 115 deny tcp any 10.0.1.0 eq telnet`
C. `access-list 115 deny udp any 10.0.1.0 eq 23`
D. `access-list 115 deny tcp any 10.0.1.0 0.0.0.255 eq 23`
E. `access-list 15 deny telnet any 10.0.1.0 0.0.0.255 eq 23`

Respuesta: D
Página: 202

345. ¿Qué utiliza el Protocolo de Árbol de Expansión para determinar el puerto designado en un puente, en una red que ejecuta STP?

A. Prioridad.
B. Coste de los enlaces conectados al switch.
C. Dirección MAC.
D. Dirección IP.

Respuesta: E
Página: 223

346. El jefe le comenta que no puede acceder a los archivos corporativos en el servidor FTP de la compañía desde su casa. Antes podía hacerlo sin problemas. Se supone que alguien ha cambiado una lista de acceso que es la que regula el acceso a los datos corporativos. El número de la lista de acceso en cuestión es 131.

¿Qué comando le permitirá ver la lista de acceso 131?

A. `show access-list 131 details`
B. `display ip address-list 131`
C. `show access-lists 131`
D. `display access-list 131 details`

Respuesta: C
Página: 213

347. Se ha creado una lista de acceso IP extendida que se muestra en la sintaxis. Ahora ha aplicado la lista de acceso a la interfaz Ethernet 0. ¿Cuál es el resultado de esta acción?

```
Router#show access-lists
Extended IP access list 135
deny tcp any 131.107.0.0 0.0.255.255 eq 25
deny tcp any any eq telnet

Router#show ip interface ethernet0
Ethernet0 is up, line protocol is up
Internet address is 172.17.9.60/24
Broad address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is enabled
Outgoing access list is 135
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
.........................
```

A. Solo se permite la salida por Ethernet 0 al correo electrónico y los accesos vía telnet.
B. Todos los nodos en la red 172.30.24.64 tendrán permitido el correo electrónico y el acceso por telnet.
C. Todos los protocolos TCP tienen permitido salir por Ethernet 0 excepto el correo electrónico y telnet.
D. Todo el tráfico IP que quiera salir por Ethernet 0 será denegado.
E. La lista de acceso está numerada incorrectamente y fallará.

Respuesta: D
Página: 214

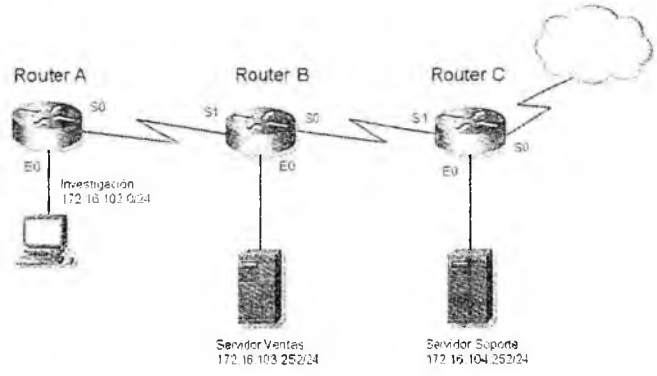
Toda lista de acceso debe incluir al menos una instrucción permit. En caso contrario, todo el tráfico será denegado.

348. Utilizando una dirección de red clase C, se necesitan 5 subredes con un máximo de 17 nodos en cada una de esas subredes. ¿Qué máscara de subred deberá utilizar?

A. 255.255.255.192
B. 255.255.255.224
C. 255.255.255.240
D. 255.255.255.248

Respuesta: B
Página: 71

349. Usted es el administrador de la red que se muestra a continuación. Se ha creado una lista de acceso nombrada "Intranet" para prevenir que usuarios de la red de Investigaciones y otros que accedan desde Internet puedan acceder al servidor de Soporte. Todos los demás usuarios de la empresa pueden tener acceso a este servidor.



La lista contiene las siguientes sentencias:

```
deny 172.16.102.0 0.0.0.255 172.16.104.252 0.0.0.0
Permit 172.16.0.0 0.0.255.255 172.16.104.252 0.0.0.0
```

¿Cuál de las siguientes secuencias de comandos permitirán colocar esta lista de modo tal que se cumplan los requerimientos enunciados?

A.
```
Router_A(config)#interface e0
Router_A(config-if)#ip access-group Intranet in
```
B.
```
Router_A(config)#interface s0
Router_A(config-if)#ip access-group Intranet out
```
C.
```
Router_B(config)#interface s0
Router_B(config-if)#ip access-group Intranet out
```
D.
```
Router_B(config)#interface s1
Router_B(config-if)#ip access-group Intranet in
```
E.
```
Router_C(config)#interface s1
Router_C(config-if)#ip access-group Intranet in
```
F.
```
Router_C(config)#interface e0
Router_C(config-if)#ip access-group Intranet out
```

Respuesta: F
Página: 204

350. ¿Cuántos tipos de encapsulación Frame-Relay están disponibles en los routers Cisco?

A. Dos.
B. Tres.
C. Cuatro.
D. Cinco.

Respuesta: A
Página: 271

351. ¿Cuál de las siguientes tecnologías utiliza un PVC en la capa 2?

A. Dial-up.
B. RDSI.
C. Frame-Relay.
D. HDLC.

Respuesta: C
Página: 268

352. ¿Cómo se denominan las PDU de la capa de Enlace de Datos?

A. Tramas.
B. Paquetes.
C. Datagramas.
D. Transportes.
E. Segmentos.
F. Bits.

Respuesta: A
Página: 49

353. Si usted deseara visualizar los valores de DLCI configurados para su red Frame-Relay, ¿qué comando utilizaría? (elija 2).

A. `show frame-relay`
B. `show running-config`
C. `show interface serial 0`
D. `show frame-relay dlci`
E. `show frame-relay pvc`

Respuesta: B, E
Página: 278

354. ¿Qué comando presentará una lista de todos los PVC y DLCI configurados en un router Cisco?

A. `show frame-relay pvc`
B. `show frame-relay`
C. `show frame-relay lmi`
D. `show pvc`

Respuesta: A
Página: 278

355. ¿Cuál de los siguientes es un método utilizado por Frame-Relay para mapear los PVC a las direcciones IP?

A. ARP.
B. LMI.
C. SLARP.
D. DLCI.

Respuesta: D
Página: 268

356. ¿Cuál es la encapsulación por defecto en enlaces punto a punto entre dos routers Cisco?

A. SDLC.
B. HDLC.
C. Cisco.
D. ANSI.

Respuesta: B
Página: 254

357. Usted trabaja como administrador de la red de la empresa. Está configurando un enlace WAN. ¿Cuáles son encapsulaciones de capa 2 típicas para este tipo de enlaces? (elija 3).

A. Ethernet.
B. Frame-Relay.
C. POTS.
D. HDLC.
E. PPP.
F. Token Ring.

Respuesta: B, D, E
Página: 106, 254

358. ¿Qué información es proporcionada por la Interfaz de Gestión Local? (elija 3).

A. El estado de los circuitos virtuales.
B. Los valores DLCI actuales.
C. El significado global o local de los valores DLCI.
D. El tipo de encapsulación LMI.

Respuesta: A, B, C
Página: 269

359. ¿En qué capa del modelo OSI tiene lugar la segmentación de un flujo de datos?

A. Física.
B. Enlace de datos.
C. Red.
D. Transporte.
E. Distribución.
F. Acceso.

Respuesta: D
Página: 23

360. ¿Qué protocolo utilizado en PPP permite el uso de múltiples protocolos de capa de red durante una conexión?

A. LCP.
B. NCP.
C. HDLC.
D. X.25.

Respuesta: B
Página: 257

361. Usted se encuentra desarrollando tareas de técnico de redes. Se le ha requerido que resuelva un fallo en el enlace WAN entre la oficina principal de la empresa localizada en Madrid y una oficina remota localizada en Oporto. Un router Cisco estaba proveyendo conectividad Frame-Relay en el sitio de Oporto, ha sido reemplazado con un router Frame-Relay de otro fabricante. Se ha perdido la conectividad entre ambos sitios

¿Cuál es más probablemente la causa del problema?

A. Falta de coincidencia en el tipo de LMI.
B. DLCI incorrecto.
C. Falta de coincidencia en el tipo de encapsulación.
D. Incorrecto mapeo de la dirección IP.

Respuesta: A
Página: 270

362. ¿Cuáles de las siguientes son características de PPP? (elija 3).

A. Puede ser utilizado sobre circuitos asincrónicos.
B. Mapea capa 2 a direcciones de capa 3.
C. Encapsula diversos protocolos enrutados.
D. Soporta solamente IP.
E. Provee mecanismos de corrección de errores.

Respuesta: A, C, E
Página: 257

363. ¿Qué rango de direcciones IP puede utilizarse en el primer octeto de una dirección de red Clase B?

A. 1-126
B. 1-127
C. 128-190

D. 128-191
E. 129-192
F. 192-220

Respuesta: D
Página: 67

364. Ha sido convocado como consultor por una compañía en rápido crecimiento y que tiene en este momento una casa central y 3 oficinas regionales. El responsable de la red está estudiando la posibilidad de implementación de una tecnología WAN escalable. Los planes actuales de la empresa incluyen la apertura de 7 oficinas regionales adicionales con requerimientos de conectividad full time. El router actualmente instalado en la casa central no dispone de puertos libres.

¿Cuál de las siguientes tecnologías es la mejor opción que le permitirá dar respuesta a las necesidades de la empresa manteniendo los costes en un nivel mínimo?

A. Enlaces dedicados con PPP o HDLC.
B. Frame-Relay.
C. ISDN-BRI.
D. ADSL.
E. Servicio de banda ancha por cable.

Respuesta: D
Página: 285

365. ¿Cómo son los extremos de un cable cruzado?

A. Los pines 1-8 son completamente opuestos en el otro extremo (8-1).
B. Tiene a los pines 1-8 cableados de igual manera en ambos extremos.
C. El pin 1 en uno de los extremos se conecta al pin 3 del otro extremo y el pin 2 se conecta al pin 6 del otro extremo.
D. El pin 2 de uno de los extremos se conecta al pin 3 del otro extremo, y el pin 1 se conecta al pin 6 en el otro extremo.

Respuesta: C
Página: 28

366. ¿En qué capa del modelo OSI se ubican los routers?

A. Física.
B. Transporte.

C. Enlace de datos.
D. Red.

Respuesta: D
Página: 37

367. ¿Cuál de las siguientes opciones es verdadera respecto a los LMIs? (elija 2).

A. Los LMIs mapean los números DLCI a los circuitos virtuales.
B. Los LMIs mapean las direcciones X.21 a los circuitos virtuales.
C. Los LMIs informan el estado de los circuitos virtuales.
D. Los mensajes LMI proporcionan información acerca del valor DLCI actual.

Respuesta: C, D
Página: 368

368. ¿Cuál de las siguientes opciones puede ser negociada utilizando LCP durante el establecimiento de un enlace PPP? (elija 2)

A. Callback.
B. IPCP.
C. CHAP.
D. Multilink.
E. TCP.
F. Q931.

Respuesta: C, D
Página: 258

369. Utilizando la dirección de clase C 192.168.21.0, necesita generar 28 subredes. ¿Qué máscara de subred deberá utilizar?

A. 255.255.0.28
B. 255.255.255.0
C. 255.255.255.28
D. 255.255.255.248
E. 255.255.255.252

Respuesta: D
Página: 71

370. ¿Cuál de los siguientes recursos contiene información de control de flujo Frame-Relay?

A. DLCI.
B. IARP.

C. LMI.
D. BECN.

Respuesta: D
Página: 269

371. Su Gerente le solicita 2 motivos para utilizar un router para segmentar la red de la Casa Central. Quisiera saber cuáles son los beneficios. ¿Qué podría indicarle como beneficios?

A. El filtrado de paquetes puede realizarse a partir de la información de capa 3.
B. Se elimina la difusión.
C. Los routers generalmente son menos costosos que los switches.
D. La difusión no se reenvía a través de los routers.
E. Agregar routers a una red disminuye la latencia.

Respuesta: A, D
Página: 37

372. ¿Que tipo de NAT utilizará para efectuar una traslación de direcciones desde varias redes internas hacia varias redes externas?

A. NAT estático.
B. NAT dinámico.
C. PAT .
D. NAT sobrecargado.

Respuesta: C, D
Página: 263

373. Se está configurando un router viejo que ejecuta una imagen antigua del IOS que no soporta ARP inverso. Si el router no soporta ARP inverso, ¿cómo puede configurar en él una conexión Frame Relay?

A. Configurando un mapa estático.
B. Definiendo una dirección IP.
C. Deshabilitando DHCP en el router Frame Relay.
D. Configurando una ruta estática hacia la red remota.

Respuesta: A
Página: 269, 272

374. Se le ha requerido que configure PPP en una interfaz de un router Cisco. ¿Cuáles son los dos métodos de autenticación que puede utilizar?

A. SSL.
B. VPN.
C. PAP.
D. LAPB.
E. CHAP.
F. SLIP.

Respuesta: C, E
Página: 258

375. Usted es el administrador de la red de la empresa y se encuentra configurando un enlace Frame-Relay en un router Cisco. ¿Cuál es el tipo por defecto de Interfaz de Administración Local transmitida por un router Cisco en un circuito Frame-Relay?

A. Q933a.
B. B8Zs.
C. IETF.
D. Cisco.
E. ANSI.

Respuesta: D
Página: 270

376. Al configurar Frame-Relay en una subinterfaz punto a punto, se ingresaron los siguientes comandos:

```
Router(config)#int s0/0
Router(config-if)#ip address 10.39.0.1 255.255.0.0
Router(config-if)#encapsulation frame-relay
Router(config-if)#interface s0/0.39 point-to-point
Router(config-subif)#frame-relay interface-dlci 139
Router(config-if)#exit
Router(config)#exit
Router#copy run start
```

¿Cuál de los siguientes elementos no debería haber sido configurado?

A. La encapculación Frame-Relay en la interfaz física.
B. El DLCI local en cada subinterfaz.
C. Una dirección IP en la interfaz física.
D. El tipo de subinterfaz como punto a punto.

Respuesta: C
Página: 273

377. El Router_A no logra conectarse con el Router_B, el cual es un dispositivo Nortel. A partir del resultado del comando show, ¿qué debería cambiar en la interfaz serie 0 del Router_A para que line protocol cambie del estado de caído a activo?

```
RouterA#show interface s0
Serial 0 is up, line protocol is down
Hardware is HD64570
Internet address 10.1.1.1
Encapsulation HDLC, loopback not set
```

A. `no shutdown`
B. `encapsulation ppp`
C. `interface serial point-to-point`
D. `clock rate 56000`

Respuesta: B
Página: 257

378. Roberto es un empleado que trabaja desde su casa brindando soporte técnico a la compañía durante las horas de la tarde. Parte de sus responsabilidades es asegurarse de que la base de datos SQL de la compañía permanezca operativa para los usuarios. Roberto utiliza para esta tarea importantes aplicaciones cliente-servidor, y realiza transferencias de grandes archivos. Adicionalmente, cuando realiza cambios, estos deben hacerse rápidamente. La compañía está preocupada acerca del coste de esta conexión y está buscando una solución práctica.

¿Qué conexión sugeriría para esta organización?

A. Una conexión ADSL para la casa del usuario.
B. Una conexión dedicada T1 para la casa del usuario.
C. Una conexión Frame-Relay dedicada para la casa del usuario.
D. Una conexión dial-up por línea estándar de 56 K para la casa del usuario.

Respuesta: A
Página: 285

379. Se ingresó el comando **debug ppp authentication**, ¿qué tipo de intercambio o saludo (handshaking) ha sido utilizado para esta sesión de PPP?

```
Router#debug ppp authentication
ppp serial1: send CHAP challenge id-47 to remote
ppp serial1: CHAP challenge from Router
ppp serial1: CHAP response received from Router
ppp serial1: CHAP response id=47 received from Router
ppp serial1: Send CHAP success id=47 to remote
ppp serial1: Remote passed CHAP authentication
ppp serial1: Passed CHAP authentication
ppp serial1: Passed CHAP authentication with remote
```

A. Una vía.
B. Doble vía.
C. Triple vía.
D. No se requiere intercambio durante la autenticación.

Respuesta: C
Página: 259

380. Jorge está teniendo dificultades para configurar subinterfaces Frame-Relay. Como administrador ha decidido enviar a Jorge un correo electrónico explicándole algunos procedimientos para la instalación. ¿Cuál de las siguientes afirmaciones debería incluir en ese correo electrónico? (elija 3).

A. Cada subinterfaz es configurada ya sea como multi-punto o como punto a punto.
B. Cualquier dirección de red debe ser removida de la interfaz física.
C. La configuración de las subinterfaces se realiza en el modo (config-if)#.
D. La encapsulación Frame-Relay debe ser configurada en cada subinterfaz.

Respuesta: A, B, C
Página: 272, 273

381. Dos routers están conectados a través de sus interfaces seriales tal como muestran las sintaxis, pero no pueden comunicarse. Se sabe que el Router_A tiene la configuración correcta. A partir de la información que se suministra, identifique el fallo en el Router_B que está causando esta pérdida de conectividad.

```
Router_A#sh int s0
Serial0 is up line protocol is down
Hardware is HD64570
Internet address is 192.168.10.1/24
MTU 1500 bytes, BW 1.433 Kbits
Reliability 255/255
```

```
Encapsulation HDLC, loopback not set
Keepalive set (10sec)


Router_B#sh int s1
Serial1 is up line protocol is down
Hardware is HD64570
Internet address is 192.168.10.2/24
MTU 1500 bytes, BW 1.433 Kbits
Reliability 255/255
Encapsulation PPP, loopback not set
Keepalive set (10sec)
LCP listen
Closed: IPCP, CDPCP
```

A. Una dirección IP incompleta.
B. Insuficiente ancho de banda.
C. Máscara de subred incorrecta.
D. Encapsulación incompatible.
E. Confiabilidad del enlace demasiado baja.
F. IPCP no activo.

Respuesta: D

En la séptima línea de ambas sintaxis se observa la encapsulación de las interfaces, en este caso son diferentes, HDLC y PPP.

382. Un técnico está instalando un teléfono IP en una nueva oficina. El teléfono y los ordenadores están conectados al mismo dispositivo. Con el fin de aprovechar el máximo de ancho de banda y que el trafico telefónico se diferencie del de datos, ¿cuál es el mejor dispositivo que el técnico puede implementar y con qué tecnología? (elija 2).

A. VLAN.
B. Subinterface.
C. STP.
D. Hub.
E. Switch.
F. Router.
G. Wireless Access Point.
H. VTP.

Respuesta: A
Página: 225

383. ¿Cual es el estándar que IEEE define para Wi-Fi?

A. IEEE 802.3
B. IEEE 802.5
C. IEEE 802.11h
D. IEEE 802.11c
E. IEEE 802.11

Respuesta: E
Página: 29, 180

384. Es necesario solucionar un problema de interferencia en la LAN inalámbrica. ¿Cuáles son los dos dispositivos que pueden interferir con el funcionamiento de esta red, ya que operan en frecuencias similares? (elija dos).

A. Microondas.
B. Radio AM.
C. Tostadora.
D. Copiadora.
E. Teléfono inalámbrico.
F. Telefonía IP.
G. I-pod.

Respuesta: A, E
Página: 184

385. ¿Qué capa del modelo Cisco proporciona segmentación de las redes de contención?

A. Acceso.
B. Física.
C. Red.
D. Distribución.
E. Principal.
F. Transporte.
G. Enlace de datos.

Respuesta: A
Página: 52

386. Si usted se encuentra tecleando comandos y recibe el siguiente mensaje,

```
Router#clock set 10:30:10
% Incomplete command
```

¿qué es lo que está mal y cómo lo arregla? (elija todas las respuestas que se apliquen).

A. El IOS no soporta un reloj en este router.
B. Esta cadena de comandos no está completa.
C. Presione la tecla flecha arriba y un signo de interrogación.
D. Presione la tecla flecha abajo y la tecla Tab.
E. Borre lo que escribió y reinicie el router.

Respuesta: B, C
Página: 128

387. ¿Cuál de los siguientes es un protocolo de estado de enlace IP?

A. RIPv2.
B. EIGRP.
C. OSPF.
D. IGRP.

Respuesta: C
Página: 168

388. Usted trabaja como auxiliar del administrador de la red. El administrador se encuentra configurando un router con interfaces tanto lógicas como físicas, y le pregunta qué factor utiliza OSPF para determinar el router ID. ¿Cuál debería ser su respuesta?

A. El menor número de red de cualquier interfaz.
B. La menor dirección IP de cualquier interfaz lógica.
C. La menor dirección IP de cualquier interfaz física.
D. El mayor número de red de cualquier interfaz
E. La mayor dirección IP de cualquier interfaz lógica.
F. La mayor dirección IP de cualquier interfaz física.

Respuesta: E
Página: 170

El router ID es un número de 32 bits utilizado por OSPF para identificar el router. Para esto se utilizan las direcciones IP del router. En principio se utiliza la dirección IP de la interfaz de loopback, si hay varias interfaces de loopback, se toma la dirección IP mayor de las interfaces loopback.

389. Al examinar la configuración de enrutamiento del Router_1 y Router_2 después de que sea enviada la próxima actualización de EIGRP desde el

Router_1 al Router_2, ¿qué rutas se mostrarán en la tabla de enrutamiento de Router_2?

```
Router_1(config)#router eigrp 200
Router_1(config-router)#network 192.168.3.0
Router_1(config-router)#network 192.168.4.0
Router_1(config-router)#network 192.168.5.0
Router_1(config-router)#network 172.16.0.0

Router_2(config)#router eigrp 300
Router_2(config-router)#network 192.168.3.0
Router_2(config-router)#network 192.168.6.0
Router_2(config-router)#network 192.168.7.0
```

A. 192.168.3.0
192.168.4.0
192.168.5.0
192.168.6.0
192.168.7.0
172.16.0.0

B. 192.168.3.0
192.168.6.0
192.168.7.0

C. 192.168.3.0
192.168.4.0
192.168.5.0
192.168.6.0
192.168.7.0

D. 172.16.0.0

E. 192.168.3.0
192.168.4.0
192.168.5.0

Respuesta: A
Página: 163

La información de enrutamiento se distribuye automáticamente dentro de diferentes AS de EIGRP y se identifican como EIGRP externo.

390. ¿Cuál de los siguientes es el rango de nodo válido para la dirección IP 192.168.168.188 255.255.255.192?

A. 192.168.168.129-190
B. 192.168.168.129-191
C. 192.168.168.128-190
D. 192.168.168.128-192

Respuesta: A
Página: 71

391. Un compañero de trabajo se encuentra estudiando el algoritmo de árbol de expansión y le acaba de preguntar cómo se determina el coste de cada ruta posible por defecto. ¿Cuál de las siguientes sería la respuesta adecuada?

A. Cuenta del número total de saltos.
B. Suma de los costes basados en el ancho de banda.
C. Se determina dinámicamente en función de la carga.
D. El coste de cada enlace individual se basa en la latencia.

Respuesta: B
Página: 223

392. ¿Qué comando muestra la información correspondiente a la opción de seguridad configurada en una interfaz?

A. `show port security [interface interface-id]`
B. `show port-security [interface interface-id]`
C. `show security port interface [interface-id]`
D. `show security-port interface [interface-id]`

Respuesta: B
Página: 238

393. ¿Cuál de los siguientes comandos encriptará su contraseña de acceso por telnet en un router Cisco?

A.
```
line telnet 0
encryption on
login
password cisxo
```

B.
```
line vty 0
password-encryption
login
password cisxo
```

C.
```
service password-encryption
line vty 0 4
login
password cisxo
```

D.
```
password-encryption
line vty 0 4
login
password cisxo
```

Respuesta: C
Página: 113, 115

394. Si se tiene la siguiente entrada de la tabla de enrutamiento, ¿cuál de los elementos que se enuncian a continuación ha sido utilizado por defecto en el cálculo del valor 1200?

```
172.16.0.0 [90/1200] via 192.168.16.3, 00:00:55, Ethernet1
```

A. MTU.
B. Ancho de banda.
C. Distancia administrativa.
D. Cuenta de saltos.
E. Métrica.
F. Retraso.

Respuesta: B, F
Página: 161, 168

395. Si desea tener más de una sesión de Telnet abierta al mismo tiempo, ¿qué combinación de teclas utilizaría para alternar de una sesión a la otra?

A. Tab + barra espaciadora.
B. Ctrl + x, luego 6.
C. Ctrl + shift + x, luego 6.
D. Ctrl + shift + 6, luego x.

Respuesta: D
Página: 142

396. Es necesario agregar un punto de acceso inalámbrico a una nueva oficina. ¿Qué otros pasos de configuración serán necesarios para conectarse al punto de acceso que ya ha sido configurado su SSID?

A. Configurar la autenticación abierta en el AP y el cliente.
B. Establecer el valor SSID públicamente en el software del cliente.
C. Establecer el valor SSID en el cliente para el SSID configurado en el AP.
D. Configuración de filtrado de direcciones MAC para permitir que el cliente se conecte al AP.
E. Ninguna de las anteriores.

Respuesta: C
Página: 189

397. ¿Cuál de los siguientes tipos de redes de datos se implementará para un usuario móvil si se requiere una tarifa de datos relativamente alta, pero a muy corta distancia?

A. Comunicación de banda ancha personal (PCS).
B. ADSL de banda ancha.
C. PAN infrarrojos.
D. Spread Spectrum.
E. LAN cable.

Respuesta: C
Página: 180

398. Un único punto de acceso 802.11g se ha configurado e instalado en el centro de una oficina. Algunos usuarios inalámbricos están experimentando lento rendimiento, mientras que la mayoría de los usuarios están operando a su máxima eficiencia.

¿Cuáles son las tres causas probables de este problema? (elija tres).

A. Nulo SSID.
B. Conflicto de cifrado TKIP.
C. Teléfonos inalámbricos.
D. Tipo u orientación de las antenas.
E. Coincidentes SSID.
F. Archivadores o armarios de metal.
G. Hornos de microondas en la sala de descanso.

Respuesta: C, D, F
Página: 184

399. Una sede corporativa cuenta con un sistema de teleconferencia que utiliza VoIP (Voz sobre IP). Este sistema utiliza UDP como el transporte de los datos. Si estos datagramas UDP llegan a su destino fuera de secuencia, ¿qué pasará?

A. UDP enviará una solicitud de información ICMP al host de origen.
B. UDP hará llegar la información en los datagramas hasta la siguiente capa del modelo OSI en el orden que lleguen.
C. UDP bajará los datagramas.
D. UDP utiliza los números de secuencia en las cabeceras de datagrama para volver a ensamblar los datos en el orden correcto.

E. UDP no se reconocen los datagramas y esperara una retransmisión de datagramas.

Respuesta: B
Página: 40

400. La WAN de su empresa está migrando de RIPv1 a RIPv2. ¿Qué tres afirmaciones son correctas sobre la versión 2 de RIP? (elija tres).

A. Se utiliza difusión de sus actualizaciones de enrutamiento.
B. Se admite la autenticación.
C. Es un protocolo de enrutamiento sin clase.
D. Tiene una distancia inferior predeterminada administrativa de RIP versión 1.
E. La cuenta máxima de saltos es la misma que la versión 1.
F. No envía la máscara de subred en actualizaciones incrementales.

Respuesta: B, C, E
Página: 151

Apéndice B

RESUMEN DE COMANDOS CISCO IOS

A continuación se detalla un listado de comandos Cisco IOS que complementan a los descritos en los capítulos anteriores.

access-list *access-list-number* {**deny** | **permit** | **remark** *line*} *source*[*source-wildcard*] [**log**]	Configura una ACL IP estándar
access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit** | **remark** *line* } *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log** | **log-input**] [**time-range** *name*]	Configura una ACL IP extendida
alias {**configure** | **exec** | **interface**} *alias-name new alias*	Crea un alias para un comando determinado
bandwidth *kilobits*	Determina el ancho de banda sobre una interfaz
banner exec *c banner-text c*	Mensaje para el modo ejecutable
banner motd *d message d*	Mensaje diario
boot system flash [*flash-fs:*] [*partition-number:*] [*filename*]	Para iniciar el IOS desde la Flash

`cdp enable`	Activa el CDP en una interfaz
`cdp run`	Activa el CDP de manera global
`clear counters` *interface-type number*	Borra todos los contadores de la interfaz
`clock rate` *speed-in-bits-per-second*	Determina el sincronismo en una interfaz DCE
`clock set` *hh:mm:ss day month year*	Configura el reloj interno
`config-register` *register-value*	Determina el registro de configuración
`copy {flash | ftp | nvram | running-config|startup-config | system | tftp} {flash | ftp | nvram | running-config | startup-config | system | tftp}`	Activa la copia según el origen y el destino
`debug all`	Inicia un proceso de depuración total
`debug ip nat`	Muestra los procesos de traslación de direcciones
`debug ip rip`	Muestra los procesos de actualización de RIP
`debug ip ospf hello`	Muestra los procesos Hello OSPF
`duplex {full | half | auto}`	Especifica la forma de operar de una interfaz
`enable password [level` *level*`] {`*password* `|` *[encryption-type] encrypted-password*`}`	Configura la enable password
`enable secret [level level] {password | [encryption-type] encrypted-password}`	Configura la enable secret
`encapsulation {dot1q | isl}` *vlan-id* `[native]`	Determina la encapsulación troncal

encapsulation { **frame-relay** | **ppp** | **slip** | **hdlc**}	Asigna el tipo de encapsulación dentro de una interfaz
erase {*filesystem:*| **start-up config**}	Elimina el contenido de la NVRAM
ip access-group *access-list-number* | *access-list-name* {**in** | **out**}	Asigna una ACL dentro de la interfaz
ip access-list extended *name*	Define una ACL extendida nombrada
ip access-list standard *name*	Define una ACL estándar nombrada
ip address *ip-address mask* [**secondary**]	Configura la dirección IP de una interfaz
ip classless	Permite recibir paquetes destinados a subredes
ip default-gateway *ip address*	Configura una puerta de enlace
ip default-network *network number*	Determina una red de último recurso
ip domain-lookup	Activa la traslación de nombre de host
ip host *name-of-host [tcp-port-number] ip-address* [*ip-address2 ... address8*]	Crea una tabla de host
ip http server	Activa la configuración desde un navegador
ip nat {**inside** | **outside**}	Determina si la interfaz es entrante o saliente en NAT
ip nat pool *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}[**type rotary**]	Crea un almacén de direcciones en NAT
ip ospf cost *cost*	Determina el coste OSPF dentro de una interfaz

ip ospf priority *number*	Determina la prioridad OSPF dentro de una interfaz
ip route *prefix mask* {*address* | *interface*} [*distance*] [**tag** *tag*] [**permanent**]	Crea una ruta estática
ip routing	Activa el enrutamiento IP
ip subnet-zero	Permite utilizar la subred cero
isdn spid1 *spid-number* [*ldn*] [*ldn2*] [*ldn3*] ... [*ldn*]	Determina el identificador del Canal I RDSI
isdn switch-type *switch-type*	Determina el tipo de switch RDSI
line [aux | console | tty | vty] *line-number* [*ending-line-number*]	Determina a qué tipo de terminal ingresar
login [**local** | **tacacs**]	Define la forma de inicio de sesión
maximum paths *maximum*	Determina la cantidad de rutas paralelas en un protocolo
media-type {**aui** | **10baset** | **100baset** | **mii**}	Define el tipo de medios de una interfaz
network *address wildcard-mask* **area** *area-id*	Define red y área en un protocolo
passive-interface *type number*	Evita envíos de actualizaciones de enrutamiento en la interfaz
ping [*protocol*] {*ip-address* | *hostname*}	Inicia el envío de paquetes ping
ppp authentication {**chap** | **chap pap** | **pap chap** | **pap**} [**if-needed**] [*list-name* | **default**] [**callin**]	Determina la autenticación PPP dentro de una interfaz

ppp chap hostname *hostname*	Define el nombre de host en PPP/chap
ppp chap password *password*	Define la contraseña en PPP/chap
redistribute *protocol* [*process-id*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**weight** *weight*] [**subnets**]	Configura la redistribución en un protocolo
router bgp as-number	Determina a BGP como protocolo de enrutamiento
router eigrp *autonomous-system*	Determina a EIGRP como protocolo de enrutamiento
router igrp *autonomous-system*	Determina a IGRP como protocolo de enrutamiento
router ospf *process-id*	Determina a OSPF como protocolo de enrutamiento
router rip	Determina a RIP como protocolo de enrutamiento
show access-lists [*access-list-number* | *access-list-name*]	Muestra todas las ACL configuradas
show cam count {**dynamic** | **static** | **permanent** | **system**} [*vlan*]	Muestra el contenido de la memoria CAM
show cdp neighbors [*type number*] [**detail**]	Muestra los vecinos CDP
show controllers serial [*number*] (2500 series)	Determina diagnósticos del estado de la interfaz
show *flash-filesystem*: [**all** | **chips** | **filesys**]	Muestra los archivos contenidos en la FLASH
show frame-relay map	Muestra los mapas Frame-Relay

show frame-relay pvc [*type number* [*dlci*]]	Muestra los PVC Frame-Relay
show hosts	Muestra la tabla de host
show interface [*interface-id* | **vlan** *number*] [**flow-control** | **pruning** | **status** | **switchport** [**allowed-vlan** | **prune-elig** | **native-vlan**]]	Muestra la información de una interfaz en un switch
show interfaces {*type number*}	Muestra la información de una interfaz
show ip arp [*ip-address*] [*hostname*] [*mac-address*] [*type number*]	Muestra una tabla ARP
show ip interface *interface-type number*	Muestra información IP de una interfaz
show ip interface brief	Muestra un resumen del estado de las interfaces
show ip nat translations [**verbose**]	Muestra las traslaciones NAT

Apéndice C

GLOSARIO

A:

ABM. Modo de Compensación Asíncrono. Modo de comunicación HDLC (y protocolo derivativo) que admite comunicaciones punto a punto orientadas a iguales entre dos estaciones, en el cual cualquiera de las estaciones puede iniciar la transmisión.

ACK. Acuse de recibo utilizado por TCP. Mensaje que se envía para confirmar que un paquete o un conjunto de paquetes ha llegado. Si el terminal de destino tiene capacidad para detectar errores, el significado de ACK es "ha llegado y además ha llegado correctamente".

ACL (*lista de control de acceso*). Lista mantenida por un router de Cisco para controlar el acceso desde o hacia un router para varios servicios (por ejemplo, para evitar que los paquetes con una dirección IP determinada salgan de una interfaz en particular del router). Ver también ACL extendida y ACL estándar.

ACL estándar (*lista de control de acceso estándar*). ACL que filtra basándose en la máscara y dirección origen. Las listas de acceso estándares autorizan o deniegan todo el conjunto de protocolos TCP/IP. Ver también ACL, ACL extendida.

ACL extendida (*lista de control de acceso extendida*). ACL que verifica las direcciones origen y destino. Comparar con ACL estándar. Ver también ACL.

Actualización del enrutamiento. Mensaje que se envía desde el router para indicar si la red es accesible y la información de coste asociada. Normalmente, las actualizaciones del enrutamiento se envían a intervalos regulares y después de que se produce un cambio en la topología de la red. Comparar con actualización relámpago.

Actualización inversa. Función de IGRP destinada a evitar grandes bucles de enrutamiento. Las actualizaciones inversas indican explícitamente que una red o subred no se puede alcanzar, en lugar de implicar que una red no se puede alcanzar al no incluirla en las actualizaciones.

Actualización relámpago. Proceso mediante el cual se envía una actualización antes de que transcurra el intervalo de actualización periódica para notificar a otros routers acerca de un cambio en la métrica.

Adaptador. Ver NIC.

Administración de errores. Una de cinco categorías de administración de red (administración de costos, de la configuración, de rendimiento y de seguridad) definidas por ISO para la administración de redes OSI. La administración de errores intenta asegurar que los fallos de la red se detecten y controlen.

Administración de red. Uso de sistemas o acciones para mantener, caracterizar o realizar el diagnóstico de fallos de una red.

Administrador de red. Persona a cargo de la operación, mantenimiento y administración de una red.

ADSL (*Asymmetric Digital Subscriber Line*). Línea Digital del Suscriptor Asimétrica. Una de las cuatro tecnologías DSL. ADSL entrega mayor ancho de banda hacia abajo (desde la oficina central al lugar del cliente) que hacia arriba (desde el lugar del cliente a la oficina central). Las tasas hacia abajo oscilan entre 1.5 a 9 Mbps, mientras que el ancho de banda hacia arriba oscila entre 16 a 640 kbps. Las transmisiones a través de ADSL funcionan a distancias de hasta 5.488 metros sobre un único par de cobre trenzado. Vea también DSL, HDSL, SDSL y VDSL.

AFP (*Protocolo de archivo AppleTalk*). Protocolo de capa de presentación que permite que los usuarios compartan archivos de datos y programas de aplicación que residen en un servidor de archivos. AFP reconoce archivos compartidos de AppleShare y Mac OS.

Alcance de cable. Intervalo de números de red válidos para su uso por parte de nodos en una red extendida AppleTalk. El valor del alcance de cable puede ser un solo número de red o una secuencia contigua de varios números de red. Las direcciones de los nodos se asignan con base en el valor de alcance de cable.

Algoritmo de árbol de extensión. Algoritmo utilizado por el Protocolo de árbol de Extensión para crear un árbol de extensión. A veces abreviado como STA.

Almacenamiento en caché. Forma de réplica en la cual la información obtenida durante una transacción anterior se utiliza para procesar transacciones posteriores.

Almacenamiento y envío. Técnica de conmutación de paquetes en la que las tramas se procesan completamente antes de enviarse al puerto apropiado. Este procesamiento incluye calcular el CRC y verificar la dirección destino. Además, las tramas se deben almacenar temporalmente hasta que los recursos de la red (como un enlace no utilizado) estén disponibles para enviar el mensaje.

Analizador de protocolo. Ver analizador de red.

Analizador de red. Dispositivo de hardware o software que le brinda diversas funciones de diagnóstico de fallos de la red, incluyendo decodificadores de paquete específicos del protocolo, pruebas de diagnóstico de fallas específicas preprogramadas, filtrado de paquetes y transmisión de paquetes.

Ancho de banda. Diferencia entre las frecuencias más altas y más bajas disponibles para las señales de red. Así mismo, la capacidad de rendimiento medida de un medio o protocolo de red determinado.

Anillo. Conexión de dos o más estaciones en una topología circular lógica. La información se pasa de forma secuencial entre estaciones activas. Token Ring, FDDI y CDDI se basan en esta topología.

Anillos dobles contrarrotantes. Topología de red en la que dos rutas de señales, cuyas direcciones son opuestas, existen en una red de transmisión de tokens. FDDI y CDDI se basan en este concepto.

ANSI (*Instituto Nacional Americano de Normalización*). Organización voluntaria compuesta por corporativas, organismos del gobierno y otros miembros que coordinan las actividades relacionadas con estándares, aprueban los estándares nacionales de los EE.UU. y desarrollan posiciones en nombre de los Estados Unidos ante organizaciones internacionales de estándares. ANSI ayuda a desarrollar estándares de los EE.UU. e internacionales en relación con, entre otras cosas, comunicaciones y networking. ANSI es miembro de la IEC (Comisión Electrotécnica Internacional) y la Organización Internacional para la Normalización.

Aplicación. Programa que ejecuta una función directamente para un usuario. Los clientes FTP y Telnet son ejemplos de aplicaciones de red.

Aplicación cliente/servidor. Aplicación que se almacena en una posición central en un servidor y a la que tienen acceso las estaciones de trabajo, lo que hace que sean fáciles de mantener y proteger.

APPN (*Internetwork avanzada de par a par*). Mejoramiento de la arquitectura original SNA de IBM. APPN maneja el establecimiento de una sesión entre nodos de iguales, cálculos de ruta transparentes y dinámicos, y priorización del tráfico APPC.

Aprendizaje de la dirección MAC. Servicio que caracteriza a un switch de aprendizaje en el que se guarda la dirección MAC origen de cada paquete recibido, de modo que los paquetes que se envían en el futuro a esa dirección se pueden enviar solamente a la interfaz de switch en la que está ubicada esa dirección. Los paquetes cuyo destino son direcciones de broadcast o multicast no reconocidas se envían desde cada interfaz de switch salvo la de origen. Este esquema ayuda a reducir el tráfico en las LAN conectadas. El aprendizaje de las direcciones MAC se define en el estándar IEEE 802.1

ARA (*Acceso Remoto AppleTalk*). Protocolo que brinda a los usuarios de Macintosh acceso directo a la información y recursos de un sitio remoto AppleTalk.

ARP (*Protocolo de Resolución de Direcciones*). Protocolo de Internet que se utiliza para asignar una dirección IP a una dirección MAC. Se define en RFC 826. Comparar con RARP.

ARP proxy (*Protocolo proxy de resolución de direcciones*). Variación del protocolo ARP en el cual un dispositivo intermedio (por ejemplo, un router) envía una respuesta ARP en nombre de un nodo final al host solicitante. ARP proxy puede reducir el uso del ancho de banda en enlaces WAN de baja velocidad.

ARPANET. Red de la Agencia de proyectos de Investigación Avanzada. Una red de conmutación de paquetes de gran importancia establecida en 1969. ARPANET fue desarrollada durante los años 70 por BBN y financiada por ARPA (y luego DARPA). Con el tiempo dio origen a Internet. El término ARPANET se declaró oficialmente en desuso en 1990.

AS (*Sistema autónomo*). Conjunto de redes bajo una administración común que comparte una estrategia de enrutamiento en común. También denominado dominio de enrutamiento. La Agencia de Asignación de Números Internet le asigna al AS un número de 16 bits.

ASBR (*Router límite de sistema autónomo*). ABR ubicado entre un sistema autónomo OSPF y una red no OSPF. Los ASBR ejecutan OSPF y otro protocolo de enrutamiento, como RIP. Los ASBR deben residir en un área OSPF no sustitutiva.

ASCII (*Código americano normalizado para el intercambio de la información*). Código de 8 bits (7 bits más paridad) para la representación de caracteres.

Asignación de direcciones. Técnica que permite que diferentes protocolos interoperen convirtiendo direcciones de un formato a otro. Por ejemplo, al enrutar IP en X.25, las direcciones IP deben asignarse a las direcciones X.25 para que la red X.25 pueda transmitir los paquetes IP.

Atenuación. Pérdida de energía de la señal de comunicación.

ATM (*Modo de Transferencia Asíncrono*). Norma internacional para la retransmisión de celdas, en la cual se transmiten múltiples tipos de servicio (como voz, vídeo o datos), en celdas de longitud fija (53 bytes). Las celdas de longitud fija permiten que el procesamiento de celdas tenga lugar en el hardware, lo que reduce los retrasos en el tránsito. ATM está diseñado para aprovechar medios de transmisión de alta velocidad como E3, SONET y T3.

ATP (*Protocolo de Transacción AppleTalk*). Protocolo a nivel de transporte que brinda un servicio de transacción libre de pérdidas entre sockets. El servicio permite intercambios entre dos clientes de sockets, donde uno de los clientes solicita al otro que realice una tarea en particular y que informe de los resultados. ATP enlaza la solicitud y la respuesta juntas para asegurar un intercambio confiable de pares de solicitud/respuesta.

AUI (*Interfaz de unidad de conexión*). Interfaz IEEE 802.3 entre una MAU y una tarjeta de interfaz de red. El término AUI también puede hacer referencia al puerto del panel posterior al que se puede conectar un cable AUI, como los que pueden encontrarse en la tarjeta de acceso Ethernet del LightStream de Cisco. También denominado cable transceptor.

AURP (*Protocolo de enrutamiento AppleTalk basado en actualización*). Método para encapsular tráfico AppleTalk en el encabezado de un protocolo ajeno, permitiendo la conexión de dos o más internetworks de redes AppleTalk no contiguas a través de una red ajena (como TCP/IP) para formar una WAN AppleTalk. Esta conexión se denomina túnel AURP. Además de su función de encapsulamiento, AURP mantiene tablas de enrutamiento para toda la WAN AppleTalk intercambiando información de enrutamiento entre routers exteriores.

Autenticación. Con respecto a la seguridad, la verificación de la identidad de una persona o proceso.

B:

Backbone. Núcleo estructural de la red, que conecta todos los componentes de la red de manera que se pueda producir la comunicación.

Balanceo de la carga. En el enrutamiento, la capacidad de un router para distribuir el tráfico a lo largo de todos sus puertos de red que están a la misma distancia desde la dirección destino. Los buenos algoritmos de balanceo de carga usan velocidad de línea e información de confiabilidad. El balanceo de carga aumenta el uso de segmentos de red, aumentando así el ancho de banda efectivo de la red.

Banda ancha. Técnica de transmisión de alta velocidad y alta capacidad que permite la transmisión integrada y simultánea de diferentes tipos de señales (voz, datos, imágenes, etc.).

Base de información de administración. Ver MIB.

BECN (*Notificación de la congestión retrospectiva*). Bit colocado por una red Frame-Relay en las tramas que viajan en sentido opuesto al de las tramas que encuentran una ruta congestionada. Los dispositivos DTE que reciben tramas con el bit BECN pueden solicitar que los niveles de protocolos más elevados tomen las medidas de control de flujo que consideren adecuadas. Ver también FECN.

BGP (*Protocolo de gateway fronterizo*). Protocolo de enrutamiento interdominios que reemplaza a EGP. BGP intercambia información de accesibilidad con otros sistemas BGP y se define en RFC 1163.

Binario. Sistema numérico compuesto por unos y ceros (1 = encendido; 0 = apagado).

BIT. Dígito binario utilizado en el sistema numérico binario. Puede ser cero o uno. Ver también byte.

BOOTP (*Protocolo Bootstrap*). Protocolo usado por un nodo de red para determinar la dirección IP de sus interfaces Ethernet para afectar al inicio de la red.

Bootstrap. Operación simple predeterminada para cargar instrucciones que a su vez hacen que se carguen otras instrucciones en la memoria o que hacen entrar a otros modos de configuración.

BPDU (*Unidad de datos de protocolo de puente*). Paquete Hello del protocolo Spanning-Tree (árbol de extensión) que se envía a intervalos configurables para intercambiar información entre los puentes de la red.

BRI (*Interfaz de Acceso Básico*). Interfaz RDSI compuesta por dos canales B y un canal D para la comunicación por un circuito conmutado de voz, vídeo y datos. Comparar con PRI.

Broadcast. Paquete de datos enviado a todos los nodos de una red. Los broadcasts se identifican por una dirección broadcast. Comparar con multicast y unicast. Ver también dirección broadcast, dominio de broadcast y tormenta de broadcast.

Bucle. Ruta donde los paquetes nunca alcanzan su destino, sino que pasan por ciclos repetidamente a través de una serie constante de nodos de red.

Bucle local. Cableado (normalmente de cables de cobre) que se extiende desde la demarcación a la oficina central del proveedor de la WAN.

Búfer de memoria. Área de la memoria donde el switch almacena los datos destino y de transmisión.

Buffer (*aprox. colchón*). Memoria intermedia que se utiliza como memoria de datos temporal durante una sesión de trabajo.

Bug (*aprox. bicho, error*). Error en el hardware o en el software que, si bien no impide la ejecución de un programa, perjudica el rendimiento del mismo al no permitir la realización de determinadas tareas o al complicar su normal funcionamiento. Esta palabra también se utiliza para referirse a un intruso.

Búsqueda de direcciones de Internet. Ver ping.

Byte. Serie de dígitos binarios consecutivos que operan como una unidad (por ejemplo, un byte de 8 bits). Ver también bit.

C:

Cable coaxial. Cable que consta de un conductor cilíndrico externo hueco, que reviste a un conductor con un solo cable interno. Actualmente se usan dos tipos de cable coaxial en las LAN: el cable de 50 ohmios, utilizado para la señalización digital, y el cable de 75 ohmios, utilizado para señales analógicas y señalización digital de alta velocidad.

Cable de fibra óptica. Medio físico que puede conducir una transmisión de luz modulada. En comparación con otros medios de transmisión, el cable de fibra óptica es más caro, pero por otra parte no es susceptible a la interferencia electromagnética, y permite obtener velocidades de datos más elevadas. A veces se denomina fibra óptica.

Cableado backbone. Cableado que brinda interconexiones entre los armarios de cableado, entre los armarios de cableado y el POP, y entre edificios que forman parte de la misma LAN.

Cableado de categoría 1. Uno de los cinco grados del cableado UTP descrito en el estándar EIA/TIA 568B. El cableado de Categoría 1 se utiliza para comunicaciones telefónicas y no es adecuado para la transmisión de datos. Ver también UTP.

Cableado de categoría 2. Uno de los cinco grados del cableado UTP descrito en el estándar EIA/TIA 568B. El cableado de Categoría 2 puede transmitir datos a velocidades de hasta 4 Mbps. Ver también UTP.

Cableado de categoría 3. Uno de los cinco grados del cableado UTP descrito en el estándar EIA/TIA 568B. El cableado de Categoría 3 se utiliza en redes 10BaseT y puede transmitir datos a velocidades de hasta 10 Mbps. Ver también UTP.

Cableado de categoría 4. Uno de los cinco grados del cableado UTP descrito en el estándar EIA/TIA 568B. El cableado de Categoría 4 se utiliza en redes Token Ring y puede transmitir datos a velocidades de hasta 16 Mbps. Ver también UTP.

Cableado de categoría 5. Uno de los cinco grados del cableado UTP descrito en el estándar EIA/TIA 568B. El cableado de Categoría 5 puede transmitir datos a velocidades de hasta 100 Mbps. Ver también UTP.

Cableado vertical. Cableado del backbone.

Caching. La tecnología caching permite que las páginas web solicitadas con mayor frecuencia por los usuarios puedan ser almacenadas en múltiples localizaciones geográficas. De esta manera, cuando un cibernauta requiere una página determinada, ésta puede bajarse desde el servidor más cercano, en lugar de hacerse desde una única computadora centralizada, localizada en algún lugar lejano del mundo. Esta tecnología permite mayores velocidades de navegación para el usuario final y ahorros en tiempos y costos.

CAM (*Memoria de contenido direccionable*). Memoria que mantiene una base de datos precisa y funcional.

Canal B (*Canal principal*). En RDSI, canal de dúplex completo de 64 kbps usado para enviar datos del usuario. Ver también 2B+D, canal D, canal E y canal H.

Canal D (*Canal de datos*). Canal RDSI, de 16 kbps (BRI) o 64 kbps (PRI), dúplex completo. Ver también canal B, canal D, canal E, y canal H.

Canal E (*Canal de eco*). Canal de control de conmutación de circuito RDSI de 64 kbps. El canal E se definió en la especificación RDSI de la UIT-T de 1984, pero se abandonó en la especificación de 1988. Comparar con canal B, canal D y canal E.

Canal H (*Canal de alta velocidad*). Canal de velocidad primaria RDSI de dúplex completo que opera a 384 kbps. Comparar con canal B, canal D y canal E.

Capa de acceso. Capa en la cual una LAN o grupo de LAN, normalmente Ethernet o Token Ring, le ofrece a los usuarios acceso frontal a los servicios de la red.

Capa de aplicación. Capa 7 del modelo de referencia OSI. Esta capa brinda servicios de red para aplicaciones del usuario. Por ejemplo, una aplicación de procesamiento de textos recibe servicios de transferencia de archivos en esta capa. Ver también modelo de referencia OSI.

Capa de control de enlace de datos. Capa 2 del modelo arquitectónico SNA. Es responsable de la transmisión de datos a través de un enlace físico en particular. Corresponde aproximadamente a la capa de enlace de datos del modelo de referencia OSI. Ver también capa de control de flujo de datos, capa de control de ruta, capa de control físico, capa de servicios de presentación, capa de servicios de transacción y capa de control de transmisión.

Capa de control de flujo de datos. Capa 5 del modelo arquitectónico SNA. Esta capa determina y maneja las interacciones entre socios de sesión, especialmente el flujo de datos. Corresponde a la capa de sesión del modelo de referencia OSI. Ver también capa de control de enlace de datos, capa de control de ruta, capa de control físico, capa de servicios de presentación, capa de servicios de transacción y capa de control de transmisión.

Capa de control de ruta. Capa 3 del modelo arquitectónico SNA. Esta capa ejecuta servicios de control secuencial relacionados con el reensamblaje adecuado de datos. La capa de control de ruta también es responsable por el enrutamiento. Equivale aproximadamente a la capa de red del modelo de referencia OSI. Ver también capa de control de flujo de datos, capa de control de enlace de datos, capa de control físico, capa de servicios de presentación, capa de servicios de transacción y capa de control de transmisión.

Capa de control de transmisión. Capa 4 en el modelo arquitectural SNA. Esta capa tiene la responsabilidad de establecer, mantener y finalizar las sesiones SNA, secuenciar mensajes de datos y controlar el flujo de nivel de sesión. Equivale a la capa de transporte del modelo de referencia OSI. Ver también capa de control de flujo de datos, capa de control de enlace de datos, capa de control de ruta, capa de control físico, capa de servicios de presentación y capa de servicios de transacción.

Capa de control físico. Capa 1 del modelo arquitectónico SNA. Esta capa es responsable por las especificaciones físicas de los enlaces físicos entre sistemas finales. Corresponde a la capa física del modelo de referencia OSI. Ver también capa de control de flujo de datos, capa de control de enlace de datos, capa de control de ruta, capa de servicios de presentación, capa de servicios de transacción y capa de control de transmisión.

Capa de distribución. Capa en la que la distribución de los servicios de red se produce en múltiples LAN en un entorno de WAN. Esta es la capa en la que se encuentra la red backbone de la WAN, normalmente basada en Fast Ethernet.

Capa de enlace. Ver capa de enlace de datos.

Capa de enlace de datos. Capa 2 del modelo de referencia. Esta capa proporciona un tránsito de datos confiable a través de un enlace físico. La capa de enlace de datos se ocupa del direccionamiento físico, topología de red, disciplina de línea, notificación de errores, entrega ordenada de las tramas y control de flujo. IEEE dividió esta capa en dos subcapas: la subcapa MAC y la subcapa LLC. A veces se denomina simplemente capa de enlace. Corresponde aproximadamente a la capa de control de enlace de datos del modelo SNA. Ver también modelo de referencia OSI.

Capa de presentación. Capa 6 del modelo de referencia OSI. Esta capa suministra representación de datos y formateo de códigos, junto con la negociación de la sintaxis de transferencia de datos. Asegura que los datos que llegan de la red puedan ser utilizados por la aplicación y garantiza que la información enviada por la aplicación pueda transmitirse a través de la red. Ver también modelo de referencia OSI.

Capa de red. Capa 3 del modelo de referencia OSI. Esta capa proporciona conectividad y selección de rutas entre dos sistemas finales. La capa de red es la capa en la que se produce el enrutamiento. Equivale aproximadamente a la capa de control de ruta del modelo SNA. Ver también modelo de referencia OSI.

Capa de servicios de presentación. Capa 6 del modelo arquitectónico SNA. Esta capa proporciona administración de recursos de red, servicios de presentación de sesión y algo de administración de aplicaciones. Equivale aproximadamente a la capa de presentación del modelo de referencia OSI.

Capa de servicios de transacción. Capa 7 en el modelo de arquitectura SNA. Representa las funciones de aplicación del usuario, por ejemplo, hojas de cálculo, procesamiento de texto o correo electrónico, mediante los cuales los usuarios interactúan con la red. Equivale aproximadamente a la capa de aplicación del modelo de referencia OSI. Ver también capa de control de flujo de datos, capa de control de enlace de datos, capa de control de ruta, capa de control físico, capa de servicios de presentación y capa de control de transmisión.

Capa de sesión. Capa 5 del modelo de referencia OSI. Esta capa establece, mantiene y administra las sesiones entre las aplicaciones. Ver también modelo de referencia OSI.

Capa de transporte. Capa 4 del modelo de referencia OSI. Esta capa segmenta y reensambla los datos dentro de una corriente de datos. La capa de transporte tiene el potencial de garantizar una conexión y ofrecer transporte confiable. Ver también modelo de referencia OSI.

Capa física. Capa 1 del modelo de referencia OSI. La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Corresponde a la capa de control físico del modelo SNA. Ver también modelo de referencia OSI.

Capa núcleo. Capa que suministra conexiones rápidas de área amplia entre sitios geográficamente remotos, uniendo una serie de redes de campus en una WAN de empresa o corporativa.

Carga. Parte de una celda, trama o paquete que contiene información de capa superior (datos).

Carga. Cantidad de actividad de un recurso de la red, como por ejemplo un router o un enlace.

Carrier común. Compañía de servicios privada, que opera bajo licencia, a cargo del suministro de servicios de comunicación al público, con tarifas reguladas.

CCITT (*Comité de Consultoría Internacional para Telefonía y Telegrafía*): Organización internacional responsable del desarrollo de estándares de comunicación. Actualmente ha pasado a llamarse UIT-T.

CDDI (*Interfaz de datos distribuidos por cobre*). Implementación de protocolos FDDI en cableado STP y UTP. CDDI transmite a distancias relativamente cortas (unos 100 metros), con velocidades de datos de 100 Mbps mediante una arquitectura de doble anillo para brindar redundancia. Se basa en el estándar dependiente del medio físico de par trenzado (TPPMD) de ANSI. Comparar con FDDI.

CDMA (*Code Division Multiple Access*). Es un término genérico que define una interfaz de aire inalámbrica basada en la tecnología de espectro extendido (spread spectrum). Para telefonía celular, CDMA es una técnica de acceso múltiple especificada por la TIA (Telecommunications Industry Association) como IS-95.

CHAP (*Protocolo de autenticación de intercambio de señales*). Función de seguridad utilizada en líneas que usan el encapsulamiento PPP para evitar el acceso no autorizado. CHAP no impide por sí mismo el acceso no autorizado, pero sí identifica el extremo remoto; el router o servidor de acceso determina entonces si se permite el acceso a ese usuario.

CIDR (*Enrutamiento sin clase entre dominios*). Técnica reconocida por BGP y basada en el agregado de rutas. CIDR permite que los routers agrupen rutas para reducir la cantidad de información de enrutamiento transportada por los routers principales. Con CIDR, un conjunto de redes IP aparece ante las redes ajenas al grupo como una entidad única de mayor tamaño.

Cifrado, codificado (*encryption*). Método para proteger los datos de un acceso no autorizado a los mismos. Se utiliza normalmente en Internet para sustraer el correo electrónico.

CIR (*Velocidad de información suscrita*). Velocidad en bits por segundo, a la que el switch Frame-Relay acepta transferir datos.

Circuito. Ruta de comunicaciones entre dos o más puntos.

Circuito asíncrono. Señal que se transmite sin sincronización precisa. Estas señales normalmente tienen diferentes frecuencias y relaciones de fases. Las transmisiones asíncronas habitualmente encapsulan caracteres individuales en bits de control (denominados bits de inicio y detención) que designan el principio y el final de cada carácter. Ver también circuito síncrono.

Circuito síncrono. Señal transmitida con sincronización precisa. Estas señales tienen la misma frecuencia, y los caracteres individuales están encapsulados en bits de control (denominados bits de arranque y bits de parada) que designan el comienzo y el fin de cada carácter.

Circuito virtual. Circuito creado para garantizar la comunicación confiable entre dos dispositivos de red. Un circuito virtual se define por un par VPI/VCI y puede ser permanente (PVC) o conmutado (SVC). Los circuitos virtuales se usan en Frame-Relay y X.25. En ATM, un circuito virtual se denomina canal virtual. A veces se abrevia VC.

Circuito virtual permanente. Ver PVC.

Cliente. Nodo o programa de software (dispositivo front-end) que requiere servicios de un servidor. Ver también servidor.

Cliente/servidor. Arquitectura de la relación entre una estación de trabajo y un servidor en una red. Comparar con par a par.

CMIP (*Protocolo de información de administración común*). Protocolo de administración de red de OSI, creado y estandarizado por ISO para el control de redes heterogéneas. Ver también CMIS.

CMIS (*Servicios de información de administración común*). Interfaz de servicio de administración de red de OSI creada y estandarizada por ISO para el control de redes heterogéneas. Ver también CMIP.

CO (*Oficina central*). Oficina local de la compañía telefónica en la cual todos los pares locales en un área determinada se conectan y donde ocurre la conmutación de circuito de las líneas del subscriptor.

Codificación. Técnicas eléctricas utilizadas para transmitir señales binarias.

Codificación. Proceso a través del cual los bits son representados por voltajes.

Cola. 1. En general, una lista ordenada de elementos a la espera de ser procesados. 2. En enrutamientos, una reserva de paquetes que esperan ser enviados por una interfaz de router.

Cola de prioridad. Función de enrutamiento en la cual se da prioridad a las tramas de una cola de salida de interfaz basándose en diversas características, tales como el protocolo, el tamaño de paquete y el tipo de interfaz.

Colisión. En Ethernet, el resultado de dos nodos que transmiten simultáneamente. Las tramas de cada dispositivo impactan y se dañan cuando se encuentran en el medio físico.

Colocación en cola. Proceso en el que las ACL pueden designar ciertos paquetes para que los procese un router antes que cualquier otro tráfico, con base en el protocolo.

Compartir la carga. Uso de dos o más rutas para enrutar paquetes al mismo destino de forma igualitaria entre múltiples routers para equilibrar el trabajo y mejorar el desempeño de la red.

Concentrador. Ver hub.

Conexión a tierra de referencia de señal. Punto de referencia que usan los dispositivos informáticos para medir y comparar las señales digitales entrantes.

Conexión doble. Topología de red en la que un dispositivo se encuentra conectado a la red a través de dos puntos de acceso independientes (puntos de conexión). Un punto de acceso es la conexión primaria, y el otro es una conexión de reserva que se activa en caso de fallo de la conexión primaria.

Conexión punto a multipunto. Uno de los dos tipos fundamentales de conexión. En ATM, una conexión punto a multipunto es una conexión unidireccional en la cual un solo sistema final de origen (denominado nodo raíz) se conecta a múltiples sistemas finales de destino (denominados hojas). Comparar con conexión punto a punto.

Conexión punto a punto. Uno de dos tipos fundamentales de conexión. En ATM, una conexión punto a punto puede ser una conexión unidireccional o bidireccional entre dos sistemas finales ATM. Comparar con conexión punto a multipunto.

Confiabilidad. Proporción entre los mensajes de actividad esperados y recibidos de un enlace. Si la relación es alta, la línea es confiable. Utilizado como métrica de enrutamiento.

Congestión. Tráfico que supera la capacidad de la red.

Conmutación. Proceso de tomar una trama entrante de una interfaz y enviarla a través de otra interfaz.

Conmutación asimétrica. Tipo de conmutación que brinda conexiones conmutadas entre puertos de ancho de banda diferente, como una combinación de puertos de 10 Mbps y 100 Mbps.

Conmutación de circuito. Sistema de conmutación en el que un circuito físico dedicado debe existir entre el emisor y el receptor durante la "llamada". Se usa ampliamente en la red de la compañía telefónica. La conmutación de circuito se puede comparar con la contención y la transmisión de tokens como método de acceso de canal y con la conmutación de mensajes y la conmutación de paquetes como técnica de conmutación.

Conmutación de paquetes. Método de networking en el cual los nodos comparten el ancho de banda entre sí enviando paquetes.

Conmutación rápida. Conmutación que ofrece el nivel más bajo de latencia, enviando inmediatamente un paquete después de recibir la dirección destino.

Conmutación sin fragmentos. Técnica de conmutación que filtra, antes de que comience el envío, los fragmentos de colisión que constituyen la mayoría de los paquetes de errores.

Consola. Equipo terminal de datos a través del cual se introducen los comandos en un host.

Contención. Método de acceso en el que los dispositivos de la red compiten para obtener permiso para acceder a un medio físico.

Control de Acceso al Medio. Ver MAC.

Control de enlace de datos síncrono. Ver SDLC.

Control de enlace lógico. Ver LLC.

Control de flujo. Técnica para garantizar que una entidad transmisora no supere la capacidad de recepción de datos de una entidad receptora. Cuando los búferes del dispositivo receptor están llenos, se envía un mensaje al dispositivo transmisor para que suspenda la transmisión hasta que se hayan procesado los datos en los búferes. En las redes IBM, esta técnica se llama pacing.

Control del flujo de ventana deslizante. Método de control de flujo en el que un receptor le da a un transmisor permiso para transmitir datos hasta que una ventana esté llena. Cuando la ventana está llena, el emisor debe dejar de transmitir hasta que el receptor publique una ventana de mayor tamaño. TCP, otros protocolos de transporte y varios otros protocolos de la capa de enlace de datos usan este método de control de flujo.

Convergencia. Velocidad y capacidad de un grupo de dispositivos de internetwork que ejecutan un protocolo de enrutamiento específico para concordar sobre la topología de una internetwork de redes después de un cambio en esa topología.

Cookie (*galleta*). Pequeño archivo que se genera en el disco duro del usuario desde una página web. Un archivo de esta clase puede registrar las actividades del usuario en la página visitada. Su uso es controvertido, puesto que implica un registro de datos en el PC del usuario.

Costo. Valor arbitrario, basado normalmente en el número de saltos, ancho de banda del medio u otras medidas, que es asignado por un administrador de red y utilizado para comparar diversas rutas a través de un entorno de internetwork de redes. Los valores de coste utilizados por los protocolos de enrutamiento determinan la ruta más favorable hacia un destino en particular: cuanto menor el coste, mejor es la ruta.

CPE (*Equipo terminal del abonado*). Equipo de terminación (por ejemplo: terminales, teléfonos y módems) proporcionados por la compañía telefónica, instalados en el sitio del cliente y conectados a la red de la compañía telefónica.

CSMA/CD (*Acceso múltiple con detección de portadora y detección de colisiones*). Mecanismo de acceso a medios dentro del cual los dispositivos que están listos para transmitir datos primero verifican el canal en busca de una portadora. El dispositivo puede transmitir si no se detecta ninguna portadora durante un período de tiempo determinado. Si dos dispositivos transmiten al mismo tiempo, se produce una colisión que es detectada por todos los dispositivos que colisionan. Esta colisión subsecuentemente demora las retransmisiones desde esos dispositivos durante un período de tiempo de duración aleatoria. El acceso CSMA/CD es utilizado por Ethernet e IEEE 802.3.

CSU/DSU (*Unidad de servicio de canal/unidad de servicio de datos*). Dispositivo de interfaz digital que conecta el equipamiento del usuario final al par telefónico digital local.

Cuenta al infinito. Problema que puede ocurrir al enrutar algoritmos que son lentos para converger, en los cuales los routers incrementan continuamente el número de saltos a redes particulares. Normalmente se impone algún número arbitrario de saltos para evitar este problema.

D:

DARPA (*Agencia de Proyectos de Investigación Avanzada para la Defensa*). Agencia gubernamental de los EE.UU. que financió la investigación y la experimentación con Internet. Antiguamente denominada ARPA, volvió a utilizar ese nombre a partir de 1994. Ver también ARPA.

DAS (*Estación de doble conexión*). Dispositivo conectado a los anillos FDDI primario y secundario. La doble conexión brinda redundancia para el anillo FDDI: si falla el anillo primario, la estación puede reiniciar el anillo primario al anillo secundario, aislando el fallo y recuperando la integridad del anillo. También denominada estación Clase A. Comparar con SAS.

Datagrama. Agrupamiento lógico de información enviada como unidad de capa de red a través de un medio de transmisión sin establecer previamente un circuito virtual. Los datagramas IP son las unidades de información primaria de Internet. Los términos celda, trama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

Datagrama IP. Unidad fundamental de información transmitida a través de Internet. Contiene direcciones origen y destino junto con datos y una serie de campos que definen cosas tales como la longitud del datagrama, la suma de verificación del encabezado y señaladores para indicar si el datagrama se puede fragmentar o ha sido fragmentado.

Datos. Datos de protocolo de capa superior.

DCE (*Equipo de transmisión de datos*). Dispositivo usado para convertir los datos del usuario del DTE en una forma aceptable para la instalación de servicios de WAN. Comparar con DTE.

DDN (*Red de Defensa de los Datos*). Red militar de los EE.UU. compuesta por una red no clasificada (MILNET) y varias redes secretas y de secreto máximo. DDN es operada y mantenida por DISA.

DDP (*Protocolo de entrega de datagramas*). Protocolo de capa de red AppleTalk responsable de la entrega socket-a-socket de datagramas en una internetwork AppleTalk.

DDR (*Enrutamiento por llamada telefónica bajo demanda*). Técnica utilizada para que un router inicie y cierre dinámicamente sesiones conmutadas por circuito a medida que las estaciones transmisoras finales las necesiten.

DECnet. Grupo de productos de comunicaciones (incluyendo un conjunto de protocolos) desarrollado y soportado por Digital Equipment Corporation. DECnet/ OSI (también denominado DECnet Fase V) es la iteración más reciente y es compatible con los protocolos OSI y protocolos Digital propietarios. Fase IV Prime brinda soporte para direcciones inherentes MAC que permiten que los nodos DECnet coexistan con sistemas que ejecutan otros protocolos que tengan restricciones de dirección MAC.

Demarcación. Punto donde termina CPE y comienza la parte del bucle local del servicio. A menudo se produce en el POP de un edificio.

Demultiplexión. Separación en múltiples corrientes de entrada que han sido multiplexadas en una señal física común en múltiples corrientes de salida. Ver también multiplexión.

Determinación de ruta. Decisión de cuál es la ruta que debe recorrer el tráfico en la nube de red. La determinación de ruta se produce en la capa de red del modelo de referencia OSI.

DHCP. Protocolo de configuración dinámica del host. Protocolo que proporciona un mecanismo para asignar direcciones IP de forma dinámica, de modo que las direcciones se pueden reutilizar automáticamente cuando los hosts ya no las necesitan.

Dial up (*marcar*). Establecer comunicación entre dos PC.

Dirección. Estructura de datos o convención lógica utilizada para identificar una entidad única, como un proceso o dispositivo de red en particular.

Dirección broadcast. Dirección especial reservada para enviar un mensaje para todas las estaciones. Por lo general, una dirección broadcast es una dirección destino MAC compuesta exclusivamente por números uno. Comparar con dirección multicast y dirección unicast. Ver también broadcast.

Dirección de capa MAC. Ver dirección MAC.

Dirección de enlace de datos. Ver dirección MAC.

Dirección de hardware. Ver dirección MAC.

Dirección de host. Ver número de host.

Dirección de presentación OSI. Dirección utilizada para ubicar una entidad de aplicación de OSI. Está compuesta por una dirección de red OSI y hasta tres selectores, uno para cada entidad de transporte, sesión y presentación.

Dirección de protocolo. Ver dirección de red.

Dirección de punto decimal. Anotación común para direcciones IP con el formato a.b.c.d, donde cada número representa, en decimales, 1 byte de la dirección IP de 4 bytes. También denominada dirección de punto o anotación punteada en cuatro partes.

Dirección de red. Dirección de capa de red que se refiere a un dispositivo de red lógico, en lugar de físico. También denominada dirección de protocolo.

Dirección de subred. Parte de una dirección IP especificada como la subred por la máscara de subred.

Dirección de zona de multicast. Dirección multicast dependiente de enlace de datos en el que un nodo recibe los broadcasts NBP dirigidos a esta zona.

Dirección del salto siguiente. Dirección IP del siguiente router en una ruta hacia determinado destino.

Dirección destino. Dirección de un dispositivo de red que recibe datos. Ver también dirección origen.

Dirección física. Ver dirección MAC.

Dirección IP. Dirección de 32 bits asignada a los hosts mediante TCP/IP. Una dirección IP corresponde a una de las cinco clases (A, B, C, D o E) y se escribe en forma de 4 octetos separados por puntos (formato decimal con punto). Cada dirección consta de un número de red, un número opcional de subred y un número de host. Los números de red y de subred se utilizan conjuntamente para el enrutamiento, mientras que el número de host se utiliza para el direccionamiento a un host individual dentro de la red o de la subred. Se utiliza una máscara de subred para extraer la información de la red y de la subred de la dirección IP. También denominada dirección de Internet (dirección IP).

Dirección MAC (*Control de Acceso al Medio*). Dirección de capa de enlace de datos estandarizada que se necesita para cada puerto o dispositivo que se conecta a una LAN. Otros dispositivos de la red usan estas direcciones para ubicar dispositivos específicos en la red y para crear y actualizar las tablas de enrutamiento y las estructuras de los datos. Las direcciones MAC tienen 6 bytes de largo y son controladas por el IEEE. También se denominan direcciones de hardware, dirección de capa MAC o dirección física. Comparar con dirección de red.

Dirección multicast. Dirección única que se refiere a múltiples dispositivos de red. Sinónimo de dirección de grupo. Comparar con dirección broadcast y dirección unicast. Ver también multicast.

Dirección origen. Dirección de un dispositivo de red que envía datos.

Dirección unicast. Dirección que especifica un solo dispositivo de red. Comparar con dirección broadcast y dirección multicast.

Direccionamiento plano. Esquema de direccionamiento que no utiliza una jerarquía lógica para determinar una ubicación.

División en capas. Separación de funciones de networking utilizadas por el modelo de referencia OSI, que simplifica las tareas requeridas para que dos PC se comuniquen entre sí.

DLCI (*identificador de conexión de enlace de datos*). Valor que especifica un PVC o un SVC en una red Frame-Relay. En la especificación Frame Relay básica, los DLCI son significativos localmente (es decir, dispositivos conectados que usan diferentes valores para especificar la misma conexión). En la especificación extendida LMI, los DLCI son significativos globalmente (es decir, los DLCI especifican dispositivos de extremos individuales).

DNS (*Sistema de denominación de dominio*). Sistema utilizado en Internet para convertir los nombres de los nodos de red en direcciones.

DoD (*Departamento de Defensa*). Organización gubernamental de los EE.UU. responsable de la defensa nacional. El Departamento de Defensa ha financiado con frecuencia el desarrollo de protocolos de comunicación.

Dominio (*domain*). Nombre empleado para referirse a una máquina o a un servidor determinado en Internet. El nombre de dominio comprende varias partes; la última parte, o sufijo, designa el nivel de estructura superior.
Ejemplos de dominios:
.com (organizaciones comerciales)
.edu (organizaciones educativas)
.gov (organizaciones gubernamentales)

Dominio de broadcast. Conjunto de todos los dispositivos que reciben tramas de broadcast que se originan en cualquier dispositivo dentro de ese conjunto. Los dominios de broadcast normalmente se encuentran limitados por routers porque los routers no envían tramas de broadcast. Ver también broadcast.

Dominio de colisión. En Ethernet, el área de la red en la que las tramas que colisionan se propagan. Los repetidores y los hubs propagan las colisiones, mientras que los switches de LAN, puentes y routers no lo hacen.

DRP (*Protocolo de Enrutamiento DECnet*). Esquema de enrutamiento propietario introducido por Digital Equipment Corporation en DECnet Fase III. En DECnet Fase V, DECnet completó su transición a los protocolos de enrutamiento OSI (ES-IS e IS-IS).

DSAP (*Punto de acceso al servicio destino*). SAP del nodo de red designado en el campo destino de un paquete. Comparar con SSAP. Ver también SAP (punto de acceso al servicio).

DSL (Digital Subscriber Line, *Línea Digital del Suscriptor*). Tecnología de red que permite conexiones de banda ancha sobre el cable de cobre a distancias limitadas. Hay cuatro tipos de DSL: ADSL, HDSL, SDSL y VDSL. Todas estas tecnologías funcionan a través de pares de módems, con un módem localizado en la oficina central y el otro en el lugar del cliente. Debido a que la mayoría de tecnologías DSL no utilizan todo el ancho de banda del par trenzado, queda espacio disponible para un canal de voz.

DTE (*Equipo terminal de datos*). Dispositivo en el extremo del usuario de una interfaz usuario a red que sirve como origen de datos, destino o ambos DTE se conecta a una red de datos a través de un dispositivo DCE (por ejemplo, un módem) y utiliza normalmente señales de sincronización generadas por el DCE. DTE incluye dispositivos tales como PC, traductores de protocolo y multiplexores. Comparar con DCE.

DWMD (*Dense Wavelength Division Multiplexing*). DWDM es una tecnología que emplea múltiples ondas para transmitir señales sobre una sola fibra óptica. Actualmente, DWDM es un componente crucial de las redes ópticas porque maximiza el uso de cables de fibra instalados y permite la entrega de servicios rápida y fácilmente sobre una infraestructura existente.

E:

E1. Esquema de transmisión digital de área amplia utilizado especialmente en Europa, que lleva datos a una velocidad de 2,048 Mbps. Las líneas E1 pueden ser dedicadas para el uso privado de carriers comunes. Comparar con T1.

E3. Esquema de transmisión digital de área amplia utilizado especialmente en Europa, que lleva datos a una velocidad de 34,368 Mbps. Las líneas E3 pueden ser dedicadas para el uso privado de carriers comunes. Comparar con T3.

EEPROM (*Memoria programable de solo lectura borrable eléctricamente*). EPROM que se puede borrar utilizando señales eléctricas aplicadas a contactos (pins) específicos.

EIA (*Asociación de Industrias Electrónicas*). Grupo que especifica los estándares de transmisiones eléctricas. EIA y TIA han desarrollado en conjunto numerosos estándares de comunicación de amplia difusión, como EIA/TIA-232 y EIA/TIA-449.

EIA/TIA568. Estándar que describe las características y aplicaciones para diversos grados de cableado UTP.

Encabezado. Información de control colocada antes de los datos al encapsularlos para la transmisión en red.

Encapsulamiento. Colocación en los datos de un encabezado de protocolo en particular. Por ejemplo, a los datos de capa superior se les coloca un encabezado específico de Ethernet antes de iniciar el tránsito de red. Además, al puentear redes que no son similares, toda la trama de una red se puede ubicar simplemente en el encabezado usado por el protocolo de capa de enlace de datos de la otra red.

Encapsular. Ver encapsulamiento.

Enlace. Canal de comunicaciones de red que se compone de un circuito o ruta de transmisión y todo el equipo relacionado entre un emisor y un receptor. Se utiliza con mayor frecuencia para referirse a una conexión de WAN. A veces se denomina línea o enlace de transmisión.

Enlace dedicado. Enlace de comunicaciones que se reserva indefinidamente para transmisiones, en lugar de conmutarse según lo requiera la transmisión. Ver también línea arrendada.

Enlace punto a punto. Enlace que proporciona una sola ruta preestablecida de comunicaciones de WAN desde las instalaciones del cliente a través de una red de carrier, como, por ejemplo, la de una compañía telefónica, a una red remota. También denominado enlace dedicado o línea arrendada.

Enlace WAN. Canal de comunicaciones de WAN que se compone de un circuito o ruta de transmisión y todo el equipo relacionado entre un emisor y un receptor.

Enrutamiento. Proceso de descubrimiento de una ruta hacia el host destino. El enrutamiento es sumamente complejo en grandes redes debido a la gran cantidad de destinos intermedios potenciales que debe atravesar un paquete antes de llegar al host destino.

Enrutamiento del camino más corto. Enrutamiento que reduce al mínimo la distancia o costo de la ruta a través de una aplicación de un algoritmo.

Enrutamiento dinámico. Enrutamiento que se ajusta automáticamente a la topología de la red o a los cambios de tráfico. También denominado enrutamiento adaptable. Comparar con enrutamiento estático.

Enrutamiento estático. Ruta que se ha configurado e introducido explícitamente en la tabla de enrutamiento. Las rutas estáticas tienen prioridad sobre las rutas elegidas por los protocolos de enrutamiento dinámico. Comparar con enrutamiento dinámico.

Enrutamiento multiprotocolo. Enrutamiento en el que un router entrega paquetes desde distintos protocolos enrutados, como TCP/IP e IPX, en los mismos enlaces de datos.

Enrutamiento por llamada telefónica bajo demanda Ver DDR.

Envío. Proceso para enviar una trama hacia su destino final mediante un dispositivo de internetwork.

Envío de tramas. Mecanismo a través del cual el tráfico basado en tramas, como HDLC y SDLC, atraviesa una red ATM.

EPROM (*Memoria programable de solo lectura borrable*). Chips de memoria no volátil programados después de su fabricación y que, de ser necesario, pueden ser borrados por ciertos medios y reprogramados. Comparar con EEPROM y PROM.

ES-IS (*Sistema Final a Sistema Intermedio*). Protocolo OSI que define el modo en que los sistemas finales (hosts) se anuncian a los sistemas intermedios (routers). Ver también IS-IS.

Escalabilidad. Capacidad de una red para aumentar de tamaño sin que sea necesario realizar cambios importantes en el diseño general.

Espera. Función de IGRP que rechaza nuevas rutas para el mismo destino durante un período determinado de tiempo.

Estación con doble conexión. Ver DAS.

Estación local doble. Dispositivo conectado a múltiples concentradores FDDI para lograr redundancia.

Estación secundaria. En protocolos síncronos de bit de la capa de enlace de datos (por ejemplo, HDLC), una estación que responde a los comandos desde una estación primaria. A veces se le denomina simplemente secundaria.

Estándar. Conjunto de reglas o procedimientos de uso generalizado o de carácter oficial.

Ethernet. El método de conexión más común en las redes de área local, LAN. En el caso de Ethernet, todas las estaciones del segmento comparten el ancho de banda total, que es 10 megabits por segundo (Mbps), 100 Mbps para Fast Ethernet o 1000 Mbps para Gigabit Ethernet.

Ethernet de dúplex completo. Capacidad de transmisión simultánea de datos entre una estación emisora y una estación receptora. Comparar con Ethernet semidúplex.

Ethernet semidúplex. Capacidad de transmisión de datos en una sola dirección a la vez entre una estación transmisora y otra receptora. Comparar con Ethernet de dúplex completo.

Evaluación loopback. Prueba en la que se envían las señales y luego se dirigen de vuelta hacia su origen desde un punto a lo largo de la ruta de comunicaciones. La evaluación loopback a menudo se usa para probar la capacidad de uso de la interfaz de la red.

F:

Fast Ethernet. Cualquiera de varias especificaciones de Ethernet de 100-Mbps. Fast Ethernet ofrece un incremento de velocidad diez veces mayor que el de la especificación de Ethernet 10BaseT, aunque preserva características tales como formato de trama, mecanismos MAC y MTU. Estas similitudes permiten el uso de herramientas de administración de red y aplicaciones 10BaseT existentes en redes Fast Ethernet. Se basa en una extensión de la especificación **IEEE 802.3**. Ver también Ethernet.

FDDI (*Interfaz de datos distribuida por fibra*). Estándar de LAN, definido por ANSI X3T9.5, que especifica una red de transmisión de tokens de 100 Mbps que utiliza cable de fibra óptica, con distancias de transmisión de hasta 2 km. FDDI usa una arquitectura de anillo doble para brindar redundancia. Comparar con CDDI y FDDI II.

FDDI II. Estándar ANSI que mejora FDDI. FDDI II brinda transmisión isócrona para circuitos de datos no orientado a conexión y circuitos de voz y vídeo orientados a conexión. Comparar con FDDI.

FECN (*Notificación explícita de la congestión*). Bit colocado por una red Frame-Relay para informar a los dispositivos DTE que reciben las tramas que se produjo congestión en la ruta del origen hacia el destino. Los dispositivos DTE que reciben las tramas con el bit FECN pueden solicitar que los protocolos de más alto nivel tomen las medidas de control de flujo correspondientes. Ver también BECN.

Fibra local 4B/5B. Fibra local de 4 bytes/5 bytes. Medio físico de canal de fibra utilizado para FDDI y ATM. Admite velocidades de hasta 100 Mbps en fibra multimodo.

Fibra local 8B/10B. Fibra local de 8 bytes/10 bytes. Medio físico de canal de fibra que admite velocidades de hasta 149,76 Mbps en fibra multimodo.

Fibra local de 4 bytes/5 bytes. Ver fibra local 4B/5B.

Fibra multimodo. Fibra óptica que soporta la propagación de múltiples frecuencias de luz.

Fibra óptica. Fibra basada en el vidrio, que sustituye a los clásicos cables de cobre y permite transmitir un gran volumen de información a alta velocidad y a gran distancia. La información no se transmite mediante impulsos eléctricos, sino que se modula en una onda de luz generada por un láser.

Filtrado de tráfico local. Proceso por el cual un puente filtra (descarta) tramas cuyas direcciones MAC origen y destino se ubican en la misma interfaz en el puente, lo que evita que se envíe tráfico innecesario a través del puente. Definido en el estándar IEEE 802.1.

Filtro. En general, se refiere a un proceso o dispositivo que rastrea el tráfico de red en busca de determinadas características, por ejemplo, una dirección origen, dirección destino o protocolo y determina si debe enviar o descartar ese tráfico basándose en los criterios establecidos.

Firewall. Router o servidor de acceso, o varios routers o servidores de acceso, designados para funcionar como búfer entre redes de conexión pública y una red privada. Un router de firewall utiliza listas de acceso y otros métodos para garantizar la seguridad de la red privada.

Firmware. Instrucciones de software establecidas de forma permanente o semipermanente en la ROM.

Flooding. Técnica de transmisión de tráfico utilizada por switches y puentes, en la cual el tráfico recibido por una interfaz se envía a todas las interfaces de ese dispositivo, salvo a la interfaz desde la cual se recibió originalmente la información.

Flujo. Corriente de datos que viajan de un punto a otro a través de una red (por ejemplo, desde una estación de la LAN a otra). Se pueden transmitir varios flujos en un solo circuito.

Foro ATM. Organización internacional fundada en 1991 de forma conjunta por Cisco Systems, NET/ADAPTIVE, Northern Telecom y Sprint, con el fin de desarrollar y promover acuerdos de implementación basados en estándares para tecnología de ATM. El Foro ATM expande los estándares oficiales desarrollados por ANSI y UIT-T, y desarrolla acuerdos de implementación antes de los estándares oficiales.

Fragmentación. Proceso de dividir un paquete en unidades más pequeñas al transmitir a través de un medio de red que no puede acomodar el tamaño original del paquete.

Fragmento. Parte de un paquete mayor que se ha dividido en unidades más pequeñas. En las redes Ethernet, también se hace referencia a esto como una trama con un límite inferior al límite permitido de 64 bytes.

Frame-Relay. Protocolo conmutado de la capa de enlace de datos, de norma industrial, que administra varios circuitos virtuales utilizando un encapsulamiento HDLC entre dispositivos conectados. Frame-Relay es más eficiente que X.25, el protocolo para el cual se considera por lo general un reemplazo.

FTP (*Protocolo de Transferencia de Archivos*). Protocolo de aplicación, parte de la pila de protocolo TCP/IP, utilizado para transferir archivos entre nodos de red. FTP se define en la RFC 959.

Full dúplex. Capacidad para la transmisión simultánea de datos entre la estación emisora y la estación receptora. Comparar con semidúplex y unidireccional.

G:

Gateway. En la comunidad IP, término antiguo que se refiere a un dispositivo de enrutamiento. Actualmente, el término router se utiliza para describir nodos que desempeñan esta función, y gateway se refiere a un dispositivo especial que realiza conversión de capa de aplicación de la información de una pila de protocolo a otro. Comparar con router.
Gateway de último recurso. Router al cual se envían todos los paquetes no enrutables.

Gb (*gigabit*). Aproximadamente 1.000.000.000 de bits.

Gbps (*gigabytes por segundo*). Medida de velocidad de transferencia.

Gigabit. Ver Gb.

GNS (*Obtener Servidor Más Cercano*). Paquete de solicitud enviado por un cliente en una red IPX para ubicar el servidor activo más cercano de un tipo en particular. Un cliente de red IPX emite una solicitud GNS para pedir una respuesta directa de un servidor conectado o una respuesta de un router que le indique en qué parte de la internetwork de redes se puede ubicar el servicio. GNS es parte de IPX SAP.

GPRS (*Servicio general de paquetes por radio*). General Package Radio Service. Servicio general de paquetes por radio que permite manejar datos sobre redes celulares de una manera más eficiente.

Grupo de circuito. Agrupación de líneas seriales asociadas que unen dos puentes. Si uno de los enlaces seriales en un grupo de circuito se encuentra en el árbol de extensión para una red, cualquiera de los enlaces seriales en el grupo de circuito se puede usar para balanceo de carga. Esta estrategia de balanceo de carga evita los problemas de ordenamiento de los datos, asignando cada dirección destino a un enlace serial en particular.

GSM (*Global System for Mobile Communications*). Es un sistema global para las comunicaciones de móviles digitales celulares. El GSM usa TDMA de banda estrecha que permite 8 llamadas simultáneas sobre la misma radiofrecuencia. El GSM se introdujo en 1991, y desde finales de 1997 este servicio estuvo disponible en más de 100 países y se ha consolidado como sistema estándar en Europa y Asia.

GUI (*Interfaz gráfica del usuario*). Entorno del usuario que utiliza representaciones gráficas y textuales de las aplicaciones de entrada y salida y de la estructura jerárquica (o de otro tipo) en la que se almacena la información. Las convenciones como botones, iconos y ventanas son típicas, y varias acciones se realizan mediante un apuntador (como un ratón). Microsoft Windows y Apple Macintosh son ejemplos importantes de plataformas que usan GUI.

H:

HCC (*Interconexión horizontal*). Armario de cableado donde el cableado horizontal se conecta a un panel de conmutación conectado mediante cableado backbone al MDF.

HDLC (*Control de Enlace de Datos de Alto Nivel*). Protocolo síncrono de la capa de enlace de datos, orientado a bit, desarrollado por ISO. HDLC especifica un método de encapsulamiento de datos en enlaces síncronos seriales que utiliza caracteres de trama y sumas de comprobación.

HDSL (*High-data-rate Digital Subscriber Line*). Línea Digital del Suscriptor de alta velocidad. Una de las cuatro tecnologías DSL. HDSL entrega 1.544 Mbps de ancho de banda hacia arriba (desde el lugar del cliente a la oficina central) y hacia abajo (desde la oficina central al lugar del cliente), sobre dos pares de cobre trenzados. Debido a que HDSL ofrece velocidad T1, las compañías telefónicas han estado utilizando HDSL para entregar acceso local para servicios T1 en la medida de lo posible. El funcionamiento de HDSL está limitado a un rango de distancia de hasta 3658,5 metros. Se utilizan repetidoras de señal para ampliar el servicio. HDSL requiere dos pares trenzados. Por esta razón es utilizado principalmente para conexiones de red PBX, sistemas de circuito de carrier digitales, POP de intercambio, servidores de Internet y redes de datos privadas. Ver también DSL, ADSL, SDSL y VDSL.

Header (*cabecera*). Parte inicial de un paquete de datos a transmitir, que contiene la información sobre los puntos de origen y de destino de un envío y sobre el control de errores. Esta expresión se aplica con frecuencia, y de manera errónea, solo a envío de correo electrónico, por lo que recibe el nombre de "mailheader", pero normalmente cualquier paquete de datos que se transmite de PC a PC contiene una "header".

Herramienta de punción. Herramienta accionada por resorte que se usa para cortar y conectar cables en un jack o en un panel de conmutación.

Hexadecimal (*base 16*). Representación numérica que usa los dígitos del 0 al 9, con su significado habitual, y las letras de la A a la F, para representar dígitos hexadecimales con valores del 10 al 15. El dígito ubicado más a la derecha cuenta por uno, el siguiente por múltiplos de 16, el siguiente por 16^2=256, etc.

Horizonte dividido. Técnica de enrutamiento en la cual se impide que la información acerca de los routers salga de la interfaz del router a través de la cual se recibió la información. Las actualizaciones del horizonte dividido son útiles para evitar los bucles de enrutamiento.

Host. PC en una red. Similar a nodo, salvo que el host normalmente implica un PC, mientras que nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores y routers. Ver también nodo.

HTML (*Lenguaje de Etiquetas por Hipertexto*). Formato simple de documentos en hipertexto que usa etiquetas para indicar cómo una aplicación de visualización, como por ejemplo un navegador de la Web, debe interpretar una parte determinada de un documento.

HTTP (*Protocolo de Transferencia de Hipertexto*). Protocolo utilizado por los navegadores y servidores de la Web para transferir archivos, como archivos de texto y de gráficos.

Hub. 1. En general, dispositivo que sirve como centro de una topología en estrella. También denominado repetidor multipuerto. 2. Dispositivo de hardware o software que contiene múltiples módulos de red y equipos de red independientes pero conectados. Los hubs pueden ser activos (cuando repiten señales que se envían a través de ellos) o pasivos (cuando no repiten, sino que simplemente dividen las señales enviadas a través de ellos).

I:

IAB (*Comité de Arquitectura de Internet*). Comité de investigadores de internetwork de redes que discute temas relativos a la arquitectura de Internet. Responsables de designar una serie de grupos relacionados con Internet, como IANA, IESG e IRSG. El IAB es nombrado por los síndicos de la ISOC. Ver también IANA, IESG, IRSG e ISOC.

IANA (*Agencia de Asignación de Números Internet*). Organización que funciona bajo el auspicio de la ISOC como parte del IAB. La IANA delega la autoridad de asignar espacios de direcciones IP y nombres de dominio al InterNIC y otras organizaciones. La IANA mantiene también una base de datos de identificadores de protocolo asignados que se utilizan en la pila TCP/IP, incluyendo los números de sistemas autónomos.

ICMP (*Protocolo de mensajes de control en Internet*). Protocolo Internet de capa de red que informa de errores y brinda información relativa al procesamiento de paquetes IP. Documentado en RFC 792.

IDF (*Servicio de distribución intermedia*). Sala de comunicaciones secundaria para un edificio donde funciona una topología de networking en estrella. El IDF depende del MDF.

IEC (*Comisión Electrotécnica Internacional*). Grupo industrial que escribe y distribuye estándares para productos y componentes eléctricos.

IEEE (*Instituto de Ingeniería Eléctrica y Electrónica*). Organización profesional cuyas actividades incluyen el desarrollo de estándares de comunicaciones y redes. Los estándares de LAN de IEEE son los estándares de mayor importancia para las LAN de la actualidad.

IEEE 802.2. Protocolo de LAN de IEEE que especifica una implementación del la subcapa LLC de la capa de enlace de datos. IEEE 802.2 maneja errores, entramados, control del flujo y la interfaz de servicio de la capa de red (capa 3). Se utiliza en las LAN IEEE 802.3 e IEEE 802.5. Ver también IEEE 802.3 e IEEE 802.5.

IEEE 802.3. Protocolo IEEE para LAN que especifica la implementación de la capa física y de la subcapa MAC de la capa de enlace de datos. IEEE 802.3 utiliza el acceso CSMA/CD a varias velocidades a través de diversos medios físicos. Las extensiones del estándar IEEE 802.3 especifican implementaciones para Fast Ethernet. Las variaciones físicas de la especificación IEEE 802.3 original incluyen 10Base2, 10Base5, 10BaseF, 10BaseT y 10Broad36. Las variaciones físicas para Fast Ethernet incluyen 100BaseTX y 100BaseFX.

IEEE 802.5. Protocolo de LAN de IEEE que especifica la implementación de la capa física y la subcapa MAC de la capa de enlace de datos. IEEE 802.5 usa acceso de transmisión de tokens a 4 o 16 Mbps en cableado STP o UTP y desde el punto de vista funcional y operacional es equivalente a Token Ring de IBM. Ver también Token Ring.

IETF (*Fuerza de Tareas de Ingeniería de Internet*). Fuerza de tareas compuesta por más de 80 grupos de trabajo responsables del desarrollo de estándares de Internet. IETF opera bajo el auspicio de ISOC.

IGRP (*Protocolo de enrutamiento de gateway interior*). Protocolo desarrollado por Cisco para tratar los problemas asociados con el enrutamiento en redes heterogéneas de gran envergadura.

IGRP extendido (*Protocolo de enrutamiento de gateway interior extendido*). Versión avanzada de IGRP desarrollada por Cisco. Ofrece propiedades de convergencia y eficacia operativa superiores, y combina las ventajas de los protocolos del estado de enlace con las de los protocolos por vector distancia. Comparar con IGRP. Ver también OSPF y RIP.

Información final. Información de control añadida a los datos cuando se encapsulan para una transmisión de red. Comparar con encabezado.

Instituto de Ingenieros Eléctricos y Electrónicos. Ver IEEE.

Intercambio de paquetes de internetwork. Ver IPX.

Intercambio de Paquetes Secuenciado. Ver SPX.

Intercambio de señales. Secuencia de mensajes intercambiados entre dos o más dispositivos de red para garantizar la sincronización de transmisión antes de enviar datos del usuario.

Interconexión horizontal. Ver HCC.

Interconexión vertical. Ver VCC.

Interfaz. 1. Conexión entre dos sistemas o dispositivos. 2. En terminología de enrutamiento, una conexión de red. 3. En telefonía, un límite compartido definido por características de interconexión física comunes, características de señal y significados de las señales intercambiadas. 4. Límite entre capas adyacentes del modelo de referencia OSI.

Interfaz de Acceso Básico. Ver BRI.

Interfaz de administración local. Ver LMI.

Interfaz de datos distribuida por fibra. Ver FDDI.

Interfaz de red. Límite entre una red de carrier y una instalación de propiedad privada.

Interfaz de Red a Usuario. Ver UNI.

Internet. La internetwork de redes más grande del mundo, que conecta decenas de miles de redes de todo el mundo y con una cultura que se concentra en la investigación y estandarización basada en el uso real. Internet evolucionó en parte de ARPANET. En un determinado momento se llamó Internet DARPA, y no debe confundirse con el término general internet (minúsculas).

Internet. Abreviatura de internetwork de redes. No debe confundirse con la Internet. Ver internetwork de redes.

Internetwork. Industria dedicada a la conexión de redes entre sí. Este término se refiere a productos, procedimientos y tecnologías.

Internetwork de redes. Agrupamiento de redes interconectadas por routers y otros dispositivos que funciona (de modo general) como una sola red.

Internetwork de sistemas abiertos. Ver OSI.

InterNIC. Organización que brinda asistencia al usuario, documentación, capacitación, servicios de registro para nombres de dominio de Internet, direcciones de red y otros servicios a la comunidad de Internet. Antiguamente denominada NIC.

Interoperabilidad. Capacidad de los equipos de informática de diferentes fabricantes para comunicarse entre sí en una red.

Interrupción. Mensaje que envía un agente SNMP al NMS, a una consola o a una terminal para indicar que se ha producido un evento importante, por ejemplo, que se ha alcanzado una condición o umbral definido específicamente.

Intervalo de mensajes de actividad. Período de tiempo transcurrido entre cada mensaje de actividad enviado por un dispositivo de red.

IOS (*Sistema Operativo de Internetwork*). Ver software Cisco IOS.

IP (*Protocolo Internet*). Protocolo de capa de red de la pila TCP/IP que ofrece un servicio de internetwork de redes no orientado a conexión. El IP brinda funciones de direccionamiento, especificación del tipo de servicio, fragmentación y reensamblaje, y seguridad. Se define en RFC 791.

IPv4 (Protocolo Internet versión 4) es un protocolo de conmutación no orientado a conexión de máximo esfuerzo. Ver también IPv6.

IPSec (Protocolo de Internet Seguro). Es un conjunto de protocolos y algoritmos de seguridad diseñados para la protección del tráfico de red para trabajar con **IPv4** e **IPv6** de modo transparente o modo túnel que soporta una gran variedad de encriptaciones y autenticaciones.

IPv6 (*IP versión 6*). Reemplazo de la versión actual de IP (versión 4). IPv6 brinda soporte para identificación de flujo en el encabezado del paquete, que se puede usar para identificar flujos. Anteriormente denominado IPng (IP de próxima generación).

IPX (*Intercambio de Paquetes de Internetwork*). Protocolo de capa de red de NetWare utilizado para transferir datos desde los servidores a las estaciones de trabajo. IPX es similar a IP y XNS.

IPX de Novell. Ver IPX.

IPXWAN (*red de área amplia IPX*). Protocolo que negocia opciones de extremo a extremo para nuevos enlaces. Cuando aparece un enlace, los primeros paquetes IPX enviados son paquetes IPXWAN que negocian las opciones para el enlace. Cuando las opciones IPXWAN se determinan con éxito, comienza la transmisión IPX normal. Definido por RFC 1362.

IS-IS (*Sistema Intermedio a Sistema Intermedio*). Protocolo de enrutamiento jerárquico de estado de enlace OSI basado en el enrutamiento DECnet Fase V, en el que los IS (routers) intercambian información de enrutamiento con base en una métrica única para determinar la topología de la red. Ver también ES-IS y OSPF.

ISO (*Organización Internacional para la Normalización*). Organización internacional que tiene a su cargo una amplia gama de estándares, incluyendo aquellos referidos al networking. ISO desarrolló el modelo de referencia OSI, un modelo popular de referencia de networking.

ISOC (*Sociedad Internet*). Organización internacional sin fines de lucro fundada en 1992, que coordina la evolución y el uso de la Internet. Además la ISOC delega facultades a otros grupos relacionados con la Internet, por ejemplo el IAB. La ISOC tiene su sede en Reston, Virginia, EE.UU. Ver también IAB.

K:

kb (*kilobit*). Aproximadamente 1.000 bits.

kB (*kilobyte*). Aproximadamente 1.000 bytes.

kbps (*kilobits por segundo*). Medida de velocidad de transferencia.

kBps (*kilobytes por segundo*). Medida de velocidad de transferencia.

Kilobit. Ver kb.

Kilobits por segundo. Ver kbps.

Kilobyte. Ver kB.

Kilobytes por segundo. Ver kBps.

L:

LAN (*Red de área local*). Red de datos de alta velocidad y bajo nivel de errores que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un solo edificio u otra área geográficamente limitada. Los estándares de LAN especifican el cableado y señalización en las capas físicas y de enlace de datos del modelo OSI. Ethernet, FDDI y Token Ring son tecnologías LAN ampliamente utilizadas. Comparar con MAN y WAN. Ver también VLAN.

LAPB (*Procedimiento de Acceso al Enlace Balanceado*). Protocolo de capa de enlace de datos en la pila de protocolo X.25. LAPB es un protocolo orientado a bit derivado de HDLC. Ver también HDLC y X.25.

LAPD (*Procedimiento de Acceso al Enlace en el Canal D*). Protocolo de capa de enlace de datos RDSI para el canal D. LAPD deriva del protocolo LAPB y se diseñó primariamente para satisfacer los requisitos de señalización del acceso básico de RDSI. Definido por las Recomendaciones de UIT-T Q.920 y Q.921.

LAT (*Transporte de área Local*). Protocolo de terminal virtual de red desarrollado por Digital Equipment Corporation.

Latencia. Retardo entre el momento en que un dispositivo solicita acceso a una red y el momento en que se le concede el permiso para transmitir. Intervalo de tiempo que toma el procesamiento de una tarea.

LCP (*Protocolo de Control de Enlace*). Protocolo que proporciona un método para establecer, configurar, mantener y terminar una conexión punto a punto.

Lenguaje de Etiquetas por Hipertexto Ver HTML.

Límite de tiempo. Evento que se produce cuando un dispositivo de red espera saber lo que sucede con otro dispositivo de red dentro de un período de tiempo especificado, pero nada de esto sucede. El agotamiento del límite de tiempo resultante generalmente hace que se deba volver a transmitir la información o que se termine la sesión entre los dos dispositivos.

Línea arrendada. Línea de transmisión reservada para una portadora de comunicaciones para uso privado de un cliente. Una línea arrendada es un tipo de línea dedicada. Ver también enlace dedicado.

Línea de acceso telefónico. Circuito de comunicaciones establecido por una conexión conmutada por circuito que usa la red de la compañía telefónica.

LLC (*Control de enlace lógico*). La más alta de las dos subcapas de enlace de datos definidas por el IEEE. La subcapa LLC maneja el control de errores, control del flujo, entramado y direccionamiento de subcapa MAC. El protocolo LLC más generalizado es IEEE 802.2, que incluye variantes no orientadas a conexión y orientadas a conexión.

LMI (*Interfaz de Administración Local*). Conjunto de mejoras a la especificación básica Frame-Relay. LMI incluye soporte para un mecanismo de actividad, que verifica que los datos estén fluyendo; un mecanismo de multicast, que le ofrece al servidor de red su DLCI local y DLCI de multicast; direccionamiento global, que le ofrece a los DLCI significado global en lugar de local en

las redes Frame-Relay; y un mecanismo de estado, que proporciona un informe de estado constante sobre los DLCI que el switch conozca.

Localizador de recursos uniforme. Ver URL.

LSA (*Publicación del estado de enlace*). Paquete de broadcast utilizado por los protocolos del estado de enlace que contiene información acerca de vecinos y costes de ruta. Los LSA son utilizados por los routers receptores para mantener sus tablas de enrutamiento. A veces se denomina paquete de estado de enlace (LSP).

M:

MAC (*Control de Acceso al Medio*). Parte de la capa de enlace de datos que incluye la dirección de 6 bytes (48 bits) del origen y del destino, y el método para obtener permiso para transmitir. Ver también capa de enlace de datos y LLC.

Malla. Topología de red en la cual los dispositivos se organizan de manera administrable, segmentada, con varias interconexiones, a menudo redundantes, colocadas de forma estratégica entre los nodos de la red. Ver también malla completa y malla parcial.

Mapa de ruta. Método para controlar la redistribución de rutas entre dominios de enrutamiento.

Máscara. Ver máscara de dirección y máscara de subred.

Máscara de dirección. Combinación de bits utilizada para describir cuál es la porción de una dirección que se refiere a la red o subred y cuál es la que se refiere al host. A veces se llama simplemente máscara.

Máscara de subred. Máscara utilizada para extraer información de red y subred de la dirección IP

Máscara wildcard. Cantidad de 32 bits que se utiliza junto con una dirección IP para determinar qué bits en una dirección IP deben ser ignorados cuando se compara dicha dirección con otra dirección IP. Una máscara wildcard se especifica al configurar una ACL.

MAU (*Unidad de conexión al medio*). Dispositivo utilizado en redes Ethernet e IEEE 802.3 que proporciona una interfaz entre el puerto AUI de una estación y el medio común de Ethernet. La MAU, que puede ser incorporada a una estación, o puede ser un dispositivo separado, lleva a cabo funciones de la capa física, incluyendo la conversión de datos digitales de la interfaz Ethernet, la detección de colisiones y la inyección de bits en la red. Denominada a veces unidad de acceso al medio, también abreviada como MAU, o transceptor.

Máximo esfuerzo de entrega. Entrega que se produce cuando un sistema de red no usa un sistema sofisticado de acuse de recibo para garantizar la entrega confiable de la información.

Mb (*megabit*). Aproximadamente 1.000.000 de bits.

Megabits por segundo. Ver Mbps.

Megabyte. Ver MB.

Memoria de acceso aleatorio. Ver RAM.

Memoria flash. Almacenamiento no volátil que se puede borrar eléctricamente y reprogramar, de manera que las imágenes de software se pueden almacenar, iniciar y reescribir según sea necesario. La memoria flash fue desarrollada por Intel y se otorga bajo licencia a otras empresas de semiconductores.

Mensaje. Agrupación lógica de información de la capa de aplicación, a menudo compuesta por una cantidad de agrupaciones lógicas de las capas inferiores, por ejemplo, paquetes. Los términos datagrama, trama, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

Mensaje de actividad. Mensaje enviado por un dispositivo de red para informar a otro dispositivo de red que el circuito virtual entre ellos se mantiene activo.

Método de acceso. 1. En general, la manera en que los dispositivos de red acceden al medio de red. 2. Software dentro de un procesador SNA que controla el flujo de información a través de una red.

Método de corte. Técnica de conmutación de paquetes que hace pasar los datos por un switch de manera tal que la parte frontal de un paquete salga del switch en el puerto de salida antes de que el paquete termine de entrar al puerto de entrada. Un dispositivo que usa conmutación de paquetes por método de corte lee, procesa y envía los paquetes inmediatamente después de que se verifica la dirección destino y se determina el puerto saliente. También denominado conmutación de paquete al vuelo.

Métrica de enrutamiento. Método mediante el cual un protocolo de enrutamiento determina que una ruta es mejor que otra. Esta información se almacena en tablas de enrutamiento. Las métricas incluyen ancho de banda, coste de la comunicación, retardo, número de saltos, carga, MTU, coste de ruta y confiabilidad. A menudo denominada simplemente métrica.

MIB (*Base de Información de Administración*). Base de datos de información de administración de la red utilizada y mantenida por un protocolo de administración de la red, por ejemplo SNMP. El valor de un objeto MIB se puede modificar o recuperar mediante los comandos SNMP, generalmente a través del sistema de administración de red GUI. Los objetos MIB se organizan en una estructura de árbol que incluye las ramas públicas (estándar) y privada (propietaria).

Modelo cliente/servidor. Descripción común de los servicios de red y los procesos del usuario modelos (programas) de estos servicios. Los ejemplos incluyen el paradigma servidor de nombres/resolución de nombres del DNS y las relaciones entre servidor de archivos/archivo-cliente como NFS y hosts sin disco.

Modelo de referencia de Internetwork de Sistemas Abiertos. Ver modelo de referencia OSI.

Modelo de referencia OSI (*Modelo de referencia de internetwork de sistemas abiertos*). Modelo de arquitectura de red desarrollado por ISO e UIT-T. El modelo está compuesto por siete capas, cada una de las cuales especifica funciones de red individuales, tales como el direccionamiento, el control de flujo, el control de errores, el encapsulamiento y la transferencia confiable de mensajes. La capa inferior (la capa física) es la más cercana a la tecnología de los medios. Las dos capas inferiores se implementan en el hardware y en el software, y las cinco capas superiores se implementan solo en el software. La capa superior (la capa de aplicación) es la más cercana al usuario. El modelo de referencia OSI se usa a nivel mundial como método para la enseñanza y la comprensión de la funcionalidad de la red. Similar en algunos aspectos a SNA. Ver capa de aplicación, capa de enlace de datos, capa de red, capa física, capa de presentación, capa de sesión y capa de transporte.

Módem. Contracción de modulador y demodulador. Puesto que el PC y la red telefónica tradicional utilizan diferentes técnicas para la transmisión de datos (el PC utiliza la técnica digital, y la línea telefónica tradicional emplea la analógica), entre ambos se debe conectar un módem, que convierte la señal del PC en señal acústica, y que en el punto de destino la convierte de nuevo en señal digital.

Monitor activo. Dispositivo a cargo de las funciones de mantenimiento de una red Token Ring. Se selecciona un nodo de red para ser el monitor activo si tiene la dirección MAC más alta del anillo. El monitor activo se encarga de las tareas de mantenimiento de anillo; por ejemplo, garantiza que no se pierdan los tokens y que las tramas no circulen indefinidamente.

MPLS (Multiprotocol Label Switching, *Switching de etiquetas multiprotocolo*). MPLS es un estándar de la industria sobre el cual se basa la conmutación (switching) de etiquetas, las cuales identifican los diferentes tipos de información sobre la red. La tecnología MPLS le permite a un proveedor de servicio montar sobre su red servicios diferenciados a los cuales se tiene acceso a través del protocolo IP. MPLS permite que los usuarios tengan acceso a la red y se "matriculen" a algunos servicios específicos, sin que esto implique tener acceso a toda la red, es decir, que se garantiza la privacidad y seguridad de la información mediante la creación de redes virtuales privadas, VPN. MPLS ofrece tanto a los operadores como a los usuarios gran flexibilidad en la implementación de servicios basados en IP así como también facilidad en la implementación de múltiples esquemas de acceso y una alta disponibilidad.

MSAU (*Unidad de acceso de estación múltiple*). Concentrador de cableado al que se conectan todas las estaciones finales de una red Token Ring. La MSAU suministra una interfaz entre estos dispositivos y la interfaz Token Ring de un router. A veces abreviada MAU.

MSO (*Multiple Service Operador, Operador de servicios múltiples*). Operador de Servicios de Cable que también ofrece otros servicios, tales como datos y/o telefonía de voz.

MTU (*Unidad máxima de transmisión*). Tamaño máximo de paquete, en bytes, que puede manejar una interfaz en particular.

Multicast. Paquetes únicos copiados por una red y enviados a un conjunto de direcciones de red. Estas direcciones están especificadas en el campo de dirección del destino. Comparar con broadcast y unicast.

Multiplexión. Esquema que permite que varias señales lógicas se transmitan de forma simultánea a través de un canal físico exclusivo. Comparar con demultiplexión.

N:

NAK (*Acuse de recibo negativo*). Respuesta que se envía desde un dispositivo receptor a un dispositivo transmisor que indica que la información recibida contiene errores. Comparar con acuse de recibo.

NAT (*Traducción de direcciones de red*). Mecanismo que reduce la necesidad de tener direcciones IP exclusivas globales. NAT permite que las organizaciones cuyas direcciones no son globalmente exclusivas se conecten a la Internet transformando esas direcciones en espacio de direccionamiento enrutable global. También denominado traductor de dirección de red.

NAUN (*Vecino corriente arriba activo más cercano*). En las redes Token Ring o IEEE 802.5, el dispositivo de red corriente arriba más cercano a cualquier dispositivo que aún esté activo.

NCP (*Programa de control de red*). Programa que enruta y controla el flujo de datos entre un controlador de comunicaciones y otros recursos de red.

NetBEUI (*Interfaz de Usuario NetBIOS Extendida*). Versión mejorada del protocolo NetBIOS que usan los sistemas operativos de red (por ejemplo: LAN Manager, LAN Server, Windows for Workgroups y Windows NT). NetBEUI formaliza la trama de transporte y agrega funciones adicionales. NetBEUI implementa el protocolo OSI LLC2.

NetBIOS (*Sistema Básico de Entrada/Salida de Red*). Interfaz de programación de aplicación que usan las aplicaciones de una LAN IBM para solicitar servicios a los procesos de red de nivel inferior. Estos servicios incluyen establecimiento y finalización de sesión, así como transferencia de información.

NetWare. Popular sistema operativo de red distribuido desarrollado por Novell. Proporciona acceso remoto transparente a archivos y varios otros servicios de red distribuidos.

Networking. Interconexión de estaciones de trabajo, dispositivos periféricos (por ejemplo, impresoras, unidades de disco duro, escáneres y CD-ROM) y otros dispositivos.

NFS (*Sistema de Archivos de Red*). Se utiliza comúnmente para designar un conjunto de protocolos de sistema de archivos distribuido, desarrollado por Sun Microsystems, que permite el acceso remoto a archivos a través de una red. En realidad, NFS es simplemente un protocolo del conjunto. Los protocolos NFS incluyen RPC y XDR. Estos protocolos son parte de una arquitectura mayor que Sun denomina ONC.

NIC (*Centro de Información de Red*). Organización cuyas funciones ha asumido InterNIC. Ver InterNIC.

NIC (*Tarjeta de interfaz de red*). Tarjeta que brinda capacidades de comunicación de red hacia y desde un PC. También denominada adaptador.

NLM (*Módulo Cargable NetWare*). Programa individual que se puede cargar en la memoria y que funciona como parte del sistema operativo de red NetWare.

NLSP (*Protocolo de Servicios de Enlace de NetWare*). Protocolo de enrutamiento de estado de enlace basado en IS-IS. La implementación de Cisco de NLSP también incluye variables y herramientas MIB para redistribuir el enrutamiento y la información SAP entre NLSP y otros protocolos de enrutamiento IPX.

NMS (*Sistema de administración de red*). Sistema que tiene la responsabilidad de administrar por lo menos parte de una red. Por regla general, un NMS es un PC bastante potente y bien equipado, como, por ejemplo, una estación de trabajo de ingeniería. Los NMS se comunican con los agentes para ayudar a realizar un seguimiento de las estadísticas y los recursos de la red.

No orientado a conexión. Transferencia de datos sin un circuito virtual. Comparar con orientado a conexión. Ver también circuito virtual.

Nodo. Punto final de la conexión de red o una unión que es común para dos o más líneas de una red. Los nodos pueden ser procesadores, controladores o estaciones de trabajo. Los nodos, que varían en cuanto al enrutamiento y a otras aptitudes funcionales, pueden estar interconectados mediante enlaces y sirven como puntos de control en la red. La palabra nodo a veces se utiliza de forma genérica para

hacer referencia a cualquier entidad que tenga acceso a una red y frecuentemente se utiliza de modo indistinto con la palabra dispositivo.

NOS (*Sistema operativo de red*). Sistema operativo utilizado para hacer funcionar una red, como, por ejemplo, NetWare de Novell y Windows NT.

NT1 (*Terminación de red de tipo 1*). Dispositivo que conecta el cableado RDSI del suscriptor de cuatro alambres a la instalación de bucle convencional local de dos alambres.

NT2 (*Terminación de red de tipo 2*). Dispositivo que dirige el tráfico hacia y desde distintos dispositivos del suscriptor y el NT1. El NT2 es un dispositivo inteligente que realiza conmutación y concentración.

NTP (*Protocolo de Tiempo de Red*). Protocolo desarrollado sobre el TCP que garantiza la precisión de la hora local, con referencia a los relojes de radio y atómicos ubicados en la Internet. Este protocolo puede sincronizar los relojes distribuidos en milisegundos durante períodos de tiempo prolongados.

Número de host. Parte de una dirección IP que designa a qué nodo de la subred se realiza el direccionamiento. También denominada dirección de host.

Número de la red. Parte de una dirección IP que especifica la red a la que pertenece el host.

Número de saltos. Métrica de enrutamiento utilizada para medir la distancia entre un origen y un destino. RIP utiliza el número de saltos como su métrica exclusiva.

Número de socket. Número de 8 bits que identifica a un socket. Se pueden asignar como máximo 254 números de socket en un nodo AppleTalk.

NVRAM (*RAM no volátil*). Memoria RAM que conserva su contenido cuando se apaga una unidad.

O:

Obtener servidor más cercano. Ver GNS.

Octeto. 8 bits. En networking, el término octeto se utiliza a menudo (en lugar de byte) porque algunas arquitecturas de máquina utilizan bytes que no son de 8 bits de largo.

ODI (*Interfaz Abierta de Enlace de Datos*). Especificación de Novell que suministra una interfaz estandarizada para tarjetas de interfaz de red (NIC) que permite que múltiples protocolos usen una sola NIC.

Oficina pequeña/oficina hogareña. Ver SOHO.

Orden de bytes de la red. Ordenamiento estándar de la Internet de los bytes correspondientes a valores numéricos.

Organización internacional para la normalización. Ver ISO.

Orientado a conexión. Transferencia de datos que requiere que se establezca un circuito virtual. Ver también no orientado a conexión y circuito virtual.

OSI (*Internetwork de sistemas abiertos*). Programa internacional de estandarización creado por ISO e UIT-T para desarrollar estándares de networking de datos que faciliten la interoperabilidad de equipos de varios fabricantes.

OSPF (*Primero la ruta libre más corta*). Protocolo de enrutamiento por estado de enlace jerárquico, que se ha propuesto como sucesor de RIP en la comunidad de Internet. Entre las características de OSPF se incluyen el enrutamiento de menor costo, el enrutamiento de múltiples rutas y el balanceo de carga.

OUI (*identificador exclusivo de organización*). Tres octetos asignados por el IEEE en un bloque de direcciones de LAN de 48 bits.

P:

Panel de conmutación. Conjunto de ubicaciones de pins y puertos que se pueden montar en un bastidor o en una consola en el armario de cableado. Los paneles de conmutación actúan como tableros de conmutación que conectan los cables de las estaciones de trabajo entre sí y con el exterior.

PAP (*Protocolo de Autenticación de Contraseña*). Protocolo de autenticación que permite que los PPP iguales se autentiquen entre sí. El router remoto que intenta conectarse al router local debe enviar una petición de autenticación A diferencia de CHAP, PAP pasa la contraseña y el nombre de host o nombre de usuario sin cifrar. PAP no evita el acceso no autorizado, sino que identifica el extremo remoto, el router o el servidor de acceso y determina si a ese usuario se le permite el acceso. PAP es compatible solo con las líneas PPP. Comparar con CHAP.

Papelera de bits. Destino de los bits descartados, según lo determine el router.

Paquete. Agrupación lógica de información que incluye un encabezado que contiene la información de control y (generalmente) los datos del usuario. Los paquetes se usan a menudo para referirse a las unidades de datos de capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

Paquete de temporizador. Método utilizado para asegurarse de que un cliente todavía está conectado a un servidor NetWare. Si el servidor no ha recibido un paquete de parte de un cliente durante un período de tiempo determinado, envía a dicho cliente una serie de paquetes de temporizador. Si la estación no envía ninguna respuesta a una cantidad predefinida de paquetes de temporizador, el servidor deduce que la estación ya no está conectada y cierra la conexión para dicha estación.

Paquete hello. Paquete multicast utilizado por routers que utilizan ciertos protocolos de enrutamiento para el descubrimiento y recuperación de vecinos. Los paquetes hello también indican que un cliente se encuentra aún operando y que la red está lista.

Par a par. Describe la comunicación entre implementaciones de la misma capa del modelo de referencia OSI en dos dispositivos de red distintos. Comparar con cliente/servidor.

PBX (*Central telefónica privada*). Conmutador de un teléfono analógico o digital ubicado en las instalaciones del suscriptor y que se usa para conectar redes telefónicas privadas y públicas.

PDN (*Red de datos públicos*). Red operada por el gobierno (como en el caso de Europa) o por entidades privadas para suministrar comunicaciones computacionales al público, generalmente

cobrando una tarifa. Las PDN permiten que las pequeñas organizaciones creen una WAN sin los costos de equipamiento de los circuitos de larga distancia.

PDU (*Unidad de datos de protocolo*). Término OSI equivalente a paquete.

PHY. 1. Subcapa física. Una de las dos subcapas de la capa física de FDDI. 2. Capa física. En ATM, la capa física se encarga de la transmisión de celdas a través de un medio físico que conecta dos dispositivos ATM. La PHY está compuesta por dos subcapas: PMD y TC.

Pico de tensión. Cualquier aumento de voltaje por encima del 110% del voltaje normal transportado por una línea de alimentación eléctrica.

Pila de protocolo. Conjunto de protocolos de comunicación relacionados entre sí que operan de forma conjunta y, como grupo, dirigen la comunicación a alguna o a todas las siete capas del modelo de referencia OSI. No todas las pilas de protocolo abarcan cada capa del modelo, y a menudo un solo protocolo de la pila se refiere a varias capas a la vez. TCP/IP es una pila de protocolo típico.

Ping (*Búsqueda de direcciones de Internet*). Mensaje de eco ICMP y su respuesta. A menudo se usa en redes IP para probar el alcance de un dispositivo de red.

Plan de distribución. Diagrama simple que indica la ubicación de los tendidos de cables y los números de las habitaciones a los que se dirigen.

PLP (*Protocolo a nivel de paquete*). Protocolo de capa de red en la pila de protocolo X.25. Algunas veces denominado X.25 Nivel 3 y protocolo X.25. Ver también X.25.

POP (*Punto de presencia*). Punto de interconexión entre las instalaciones de comunicación suministradas por la compañía telefónica y el servicio de distribución principal del edificio.

Portadora. Onda electromagnética o corriente alterna de una sola frecuencia, adecuada para modulación por parte de otra señal portadora de datos.

POST (*Pruebas al inicio*). Conjunto de diagnósticos de hardware que se ejecutan en un dispositivo de hardware cuando se enciende.

Postergación. Retardo en la retransmisión que se produce cuando tiene lugar una colisión.

PPP (*Protocolo Punto a Punto*). Sucesor del SLIP, un protocolo que suministra conexiones router a router y host a red a través de circuitos síncronos y asíncronos.

PRI (*Interfaz de Acceso Principal*). Interfaz RDSI al acceso principal. El acceso principal consta de un canal D único de 64 Kbps más 23 canales B (T1) o 30 canales B (E1) para voz o datos. Comparar con BRI.

Primero la ruta libre más corta. Ver OSPF.

PROM (*Memoria programable de solo lectura*). ROM que puede programarse utilizando equipo especial. Las PROM pueden ser programadas solamente una vez. Comparar con EPROM.

Protocolo. Descripción formal de un conjunto de normas y convenciones que establecen la forma en que los dispositivos de una red intercambian información.

Protocolo Bootstrap. Ver BOOTP.

Protocolo de árbol de expansión. Protocolo puente que utiliza el algoritmo de árbol de expansión, lo que habilita un puente de aprendizaje para funcionar dinámicamente en torno de bucles en una topología de red creando un árbol de expansión. Los puentes intercambian mensajes BPDU con otros puentes para detectar bucles y luego eliminarlos al desactivar las interfaces de puente seleccionadas. Se refiere tanto al estándar IEEE 802.1 de Protocolo de árbol de expansión, como al Protocolo de árbol de expansión más antiguo, de Digital Equipment Corporation, en el cual se basa. La versión de IEEE admite dominios de puente y permite que el puente desarrolle una topología sin bucles a través de una LAN.

Protocolo de enrutamiento. Protocolo que logra el enrutamiento mediante la implementación de un protocolo de enrutamiento específico. Entre los ejemplos de protocolo de enrutamiento se incluyen IGRP, OSPF y RIP. Comparar con protocolo enrutado.

Protocolo de enrutamiento DECnet. Ver DRP.

Protocolo de enrutamiento híbrido balanceado. Protocolo que combina aspectos de los protocolos de estado de enlace y por vector distancia. Ver también protocolo de enrutamiento de estado de enlace y protocolo de enrutamiento por vector distancia.

Protocolo de enrutamiento por estado de enlace. Protocolo de enrutamiento en el cual cada router realiza un broadcast o multicast de información referente al coste de alcanzar cada uno de sus vecinos a todos los nodos de la internetwork de redes. Los protocolos de estado de enlace crean una vista coherente de la red y por lo tanto no son propensos a bucles de enrutamiento, pero por otro lado para lograr esto deben sufrir dificultades informáticas relativamente mayores y un tráfico más diseminado (comparado con los protocolos de enrutamiento por vector distancia). Comparar con protocolo de enrutamiento híbrido balanceado y protocolo de enrutamiento por vector de distancia.

Protocolo de enrutamiento por vector distancia. Protocolo que itera en el número de saltos en una ruta para encontrar el árbol de extensión de ruta más corta. Los protocolos de enrutamiento por vector distancia piden a cada router que envíe su tabla de enrutamiento completa en cada actualización, pero solamente a sus vecinos. Los algoritmos de enrutamiento por vector distancia pueden ser propensos a los bucles de enrutamiento, pero desde el punto de vista informático son más simples que los algoritmos de enrutamiento de estado de enlace. También denominado algoritmo de enrutamiento Bellman-Ford. Comparar con el protocolo de enrutamiento híbrido balanceado y el protocolo de enrutamiento del estado de enlace.

Protocolo enrutado. Protocolo que puede ser enrutado por el router. Un router debe ser capaz de interpretar la internetwork de redes lógica según lo que especifique dicho protocolo enrutado. AppleTalk, DECnet e IP son ejemplos de protocolos enrutados. Comparar con protocolo de enrutamiento.

Protocolo exterior. Protocolo utilizado para intercambiar información de enrutamiento entre redes que no comparten una administración común. Comparar con protocolo interior.

Protocolo interior. Protocolo utilizado para enrutar redes que se encuentran bajo una administración de red común.

Protocolo Internet. Cualquier protocolo que forme parte de la pila de protocolo TCP/IP. Ver IP. Ver también TCP/IP.

Protocolo Internet. Ver IP.

Protocolo proxy de resolución de direcciones. Ver ARP proxy.

Protocolo punto a punto. Ver PPP.

Protocolo SPF (*Primero la ruta más corta*). Algoritmo de enrutamiento que itera sobre la longitud de la ruta para determinar el árbol de extensión de la ruta más corta. Comúnmente empleado en los algoritmos de enrutamiento de estado de enlace. A veces denominado algoritmo de Dijkstra.

Proveedor de acceso (*Access provider*). Cualquier organización comercial o privada que ofrece acceso a Internet o a un servicio de esta red, por ejemplo, al correo electrónico (e-mail).

Proxy. Entidad que, para aumentar la eficiencia, esencialmente reemplaza a otra entidad.

PTT (*Administración postal, de telégrafos y de teléfonos*). Agencia gubernamental que brinda servicios telefónicos. Las PTT existen en la mayoría de las áreas fuera de América del Norte y brinda servicios telefónicos tanto locales como de larga distancia.

Publicación. Proceso de router en el que las actualizaciones de servicio o enrutamiento se envían de tal manera que otros routers de la red puedan mantener listas de rutas utilizables.

Puente. Dispositivo que conecta y transmite paquetes entre dos segmentos de red que usan el mismo protocolo de comunicaciones. Los puentes operan en la capa de enlace de datos (capa 2) del modelo de referencia OSI. En general, un puente filtra, envía o realiza un flooding de una trama entrante con base en la dirección MAC de esa trama.

Puenteado. Tecnología en la que un puente conecta dos o más segmentos de LAN.

Puerto. 1. Interfaz en un dispositivo de internetwork (por ejemplo, un router). 2. Enchufe hembra en un panel de conmutación que acepta un enchufe macho del mismo tamaño, como un jack RJ-45. En estos puertos se usan los cables de conmutación para interconectar PC conectados al panel de conmutación. Esta interconexión permite que la LAN funcione. 3. En la terminología IP, un proceso de capa superior que recibe información de las capas inferiores. Los puertos tienen un número, y muchos de ellos están asociados a un proceso específico. Por ejemplo, SMTP está asociado con el puerto 25. Un número de puerto de este tipo se denomina dirección conocida. 4. Volver a escribir el software o el microcódigo para que se ejecute en una plataforma de hardware o en un entorno de software distintos de aquellos para los que fueron diseñados originalmente.

Punto de acceso al servicio. Campo definido por la especificación IEEE 802.2 que forma parte de una especificación de dirección.

Punto de acceso al servicio destino. Ver DSAP.

Punto de referencia. Especificación que define la conexión entre dispositivos específicos, según sea su función en la conexión de extremo a extremo.

PVC (*Circuito virtual permanente*). Circuito virtual que se establece de forma permanente. Los PVC ahorran el ancho de banda relacionado con el establecimiento y el desmantelamiento del circuito en situaciones en las que ciertos circuitos virtuales deben existir de forma permanente. Comparar con SVC.

Q:

Q.931. Protocolo que recomienda una capa de red entre el extremo final de la terminal y el switch RDSI local. Q.931 no impone una recomendación de extremo a extremo. Los diversos proveedores y tipos de switch de RDSI pueden usar varias implementaciones de Q.931.

QoS (*Calidad de servicio*). Medida de desempeño de un sistema de transmisión que refleja su calidad de transmisión y disponibilidad de servicio.

R:

RAM (*Memoria de acceso aleatorio*). Memoria volátil que puede ser leída y escrita por un microprocesador.

RARP (*Protocolo de Resolución Inversa de Dirección*). Protocolo en la pila TCP/ IP que brinda un método para encontrar direcciones IP con base en las direcciones MAC. Comparar con ARP.

RDSI (*Red digital de servicios integrados*). Protocolo de comunicaciones que ofrecen las compañías telefónicas y que permite que las redes telefónicas transmitan datos, voz y tráfico de otros orígenes.

Red. Agrupación de PC, impresoras, routers, switches y otros dispositivos que se pueden comunicar entre sí a través de algún medio de transmisión.

Red de área local. Ver LAN.

Red de área local en bus con paso de token. Arquitectura de LAN que usa la transmisión de tokens en una topología de bus. Esta arquitectura de LAN es la base de la especificación de LAN IEEE 802.4.

Red digital de servicios integrados. Ver RDSI.

Red empresaria. La red de una asociación comercial, agencia, escuela u otra organización que une sus datos, comunicaciones, informática y servidores de archivo.

Red híbrida. Internetwork de redes compuesta por más de un tipo de tecnología de red, incluyendo LAN y WAN.

Red interna. Red interna a la que tienen acceso los usuarios con acceso a la LAN interna de una organización.

Red no extendida. Red AppleTalk Fase 2 que soporta direccionamiento de hasta 253 nodos y solo 1 zona.

Red plana. Red en la cual no hay routers ubicados entre los switches, los broadcasts y las transmisiones de capa 2 se envían a todos los puertos conmutados y hay un dominio de broadcast que ocupa toda la red.

Red suministrada. El conjunto de switches e instalaciones (denominadas enlaces troncales) dentro de la nube del proveedor de WAN.

Redirigido. Parte de los protocolos ICMP y ES-IS que permiten que el router le indique al host que sería más efectivo usar otro router.

Redundancia. 1. En internetwork, duplicación de dispositivos, servicios o conexiones, de modo que, en caso de que se produzca una falla, los dispositivos, servicios o conexiones redundantes puedan realizar el trabajo de aquellos en los que se produce la falla. 2. En telefonía, la porción de la información total contenida en un mensaje que se puede eliminar sin sufrir pérdidas de información o significado esencial.

Reensamblaje. Colocación en su formato original de un datagrama IP en el destino después de su fragmentación en el origen o en un nodo intermedio.

Rendimiento. Velocidad de la información que llega a, y posiblemente pase a través de, un punto determinado del sistema de red.

Repetidor. Dispositivo que regenera y propaga las señales eléctricas entre dos segmentos de red.

Reserva de ancho de banda. Proceso de asignar ancho de banda a usuarios y aplicaciones que reciben servicios de una red. Involucra asignar una prioridad a diferentes flujos de tráfico según su importancia y grado de sensibilidad al retardo. Utiliza de la mejor manera posible el ancho de banda disponible y, si la red se congestiona, el tráfico de baja prioridad se descarta. A veces se denomina asignación de ancho de banda.

Resolución de direcciones. En general, un método para resolver diferencias entre esquemas de direccionamiento del computador. La resolución de direcciones habitualmente especifica un método para asignar las direcciones de capa de red (capa 3) a las direcciones de capa de enlace de datos (capa 2).

Resolución de nombre. En general, el proceso de asociación de un nombre con una dirección de red.

Resumen de ruta. La consolidación de números de red publicados en OSPF e IS-IS. En OSPF, esto hace que un resumen de ruta único se publique a otras áreas a través de un router fronterizo.

Retardo. Tiempo entre la iniciación de una transacción por parte del emisor y la primera respuesta recibida por éste. Así mismo, el tiempo requerido para mover un paquete desde el origen hasta el destino en una ruta dada.

Retardo de cola. Cantidad de tiempo que los datos deben esperar antes de poder ser transmitidos a un circuito físico multiplexado estadísticamente.

Retardo de propagación. Tiempo requerido para que los datos recorran una red, desde el origen hasta el destino final. También denominado latencia.

RFC (*petición de comentarios*). Serie de documentos empleada como medio de comunicación primario para transmitir información acerca de la Internet. Algunas RFC son designadas por el IAB como estándares de Internet. La mayoría de las RFC documentan especificaciones de protocolos tales como Telnet y FTP, pero algunas son humorísticas o históricas. Las RFC pueden encontrarse en línea en distintas fuentes.

RIP (*Protocolo de información de enrutamiento*). Protocolo suministrado con los sistemas BSD de UNIX. El Protocolo de Gateway Interior (IGP) más común de la Internet. RIP utiliza el número de saltos como métrica de enrutamiento.

RMON (*Monitoreo remoto*). Especificación del agente MIB descrita en RFC 1271 que define las funciones del monitoreo remoto de dispositivos de la red. La especificación RMON suministra varias capacidades de monitoreo, detección de problemas e informes.

ROM (*Memoria de solo lectura*). Memoria no volátil que puede ser leída, pero no escrita, por el microprocesador.

Router. Dispositivo de capa de red que usa una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes de una red a otra basándose en la información de capa. Denominado a veces gateway (aunque esta definición de gateway se está volviendo obsoleta).

Router de generación. Router de una red AppleTalk que tiene el número de red o rango de cable incorporado en el descriptor de puerto. El router de generación define el número de red o el alcance de cable para otros routers de ese segmento de la red y responde a las consultas de configuración de los routers no generadores en la red AppleTalk conectada, permitiendo que esos routers confirmen o modifiquen sus configuraciones en consecuencia. Cada red AppleTalk debe tener al menos un router de generación.

Router designado. Router OSPF que genera LSA para una red multiacceso y tiene otras responsabilidades especiales al ejecutar OSPF. Cada OSPF multiacceso, que tiene por lo menos dos routers conectados, tiene un router designado elegido por el protocolo Hello OSPF. El router designado permite una reducción en la cantidad de adyacencias requeridas en una red multiacceso, que a su vez reduce la cantidad de tráfico de protocolo de enrutamiento y el tamaño de la base de datos topológica.

Router fronterizo. Router ubicado en los bordes, o al final, de la frontera de la red, que brinda protección básica contra las redes externas, o contra un área menos controlada de la red para un área más privada de la red.

Router no generador. En AppleTalk, un router que primero debe obtener, y luego verificar, su configuración con un router de generación antes de poder comenzar a operar. Ver también router de generación.

Routers vecinos. En OSPF, dos routers que tienen interfaces a una red común. En redes multiacceso, el protocolo Hello OSPF detecta a los vecinos de forma dinámica.

RPC (*Llamada de procedimiento remoto*). Base tecnológica de la arquitectura cliente/servidor. Las RPC son llamadas de procedimiento que los clientes crean o especifican y que se ejecutan en los servidores. Los resultados se devuelven a los clientes a través de la red.

RPF (*Envío del camino inverso*). Técnica multicast en la cual un datagrama multicast se envía a todas las interfaces salvo la interfaz receptora si esta es la que se utiliza para enviar datagramas unicast hacia el origen del datagrama multicast.

RSVP (*Protocolo de reserva de recursos*). Protocolo que hace posible la reserva de recursos a través de una red IP. Las aplicaciones que se ejecutan en los sistemas finales IP pueden usar RSVP para indicarle a los otros nodos la naturaleza (ancho de banda, fluctuación de fase, ráfaga máxima, etc.) de las corrientes de paquetes que desean recibir. RSVP depende de IPv6. También denominado Protocolo de configuración de reserva de recursos.

RTMP (*Protocolo de Mantenimiento de Tabla de Enrutamiento*). Protocolo de enrutamiento propietario de Apple Computer. RTMP establece y mantiene la información de enrutamiento que se necesita para enrutar datagramas desde cualquier socket origen hacia cualquier socket destino en una red AppleTalk. Al usar RTMP, los routers mantienen las tablas de enrutamiento de forma dinámica para reflejar los cambios en la topología. RTMP deriva de RIP.

RTP (*Protocolo de Tabla de Enrutamiento*). Protocolo de enrutamiento VINES basado en RIP. Distribuye la información de la topología de red y ayuda a los servidores VINES a detectar a los clientes, servidores y routers vecinos. Usa el retardo como medida de enrutamiento.

RTP (*Protocolo de Transporte Rápido*). Protocolo que suministra control de flujo y recuperación de errores para datos APPN a medida que atraviesa la red APPN. Con RTP, la recuperación de errores y el control de flujo se realizan de extremo a extremo en lugar de en cada nodo. RTP previene la congestión, en lugar de reaccionar ante ella.

RTP (*Protocolo de Transporte en Tiempo Real*). Uno de los protocolos IPv6. RTP está diseñado para suministrar funciones de transporte de red de extremo a extremo para aplicaciones que transmiten datos de tiempo real, como, por ejemplo, datos de audio, vídeo o simulación, a través de servicios de red de multicast o de unicast. RTP suministra diversos servicios, tales como la identificación de tipo de carga, la numeración de secuencias, el uso de marca horaria y el monitoreo de entrega para aplicaciones de tiempo real.

Ruta por defecto. Una entrada de la tabla de enrutamiento que se utiliza para dirigir las tramas para las cuales el próximo salto no está explícitamente mencionado en la tabla de enrutamiento.

S:

SAI (*Sistemas de alimentación ininterrumpida*). Dispositivo de seguridad diseñado para suministrar una fuente de alimentación ininterrumpida en caso de que se produzca una interrupción del suministro de energía. Los SAI habitualmente se instalan en servidores de archivos y hubs de cableado.

Salto. Pasaje de un paquete de datos entre dos nodos de red (por ejemplo, entre dos routers).

SAP (*Protocolo de Publicación de Servicio*). Protocolo IPX que suministra un medio para informar a los clientes, a través de routers y servidores, acerca de los recursos y los servicios de red disponibles.

SAS (*Estación de una conexión*). Dispositivo conectado solo al anillo primario de un anillo FDDI. También denominada estación de Clase B. Comparar con DAS. Ver también FDDI.

SDLC (*Control Síncrono del Enlace de Datos*). Protocolo de comunicaciones de capa de enlace de datos de SNA. SDLC es un protocolo serial de dúplex completo orientado a bit que ha dado origen a numerosos protocolos similares, entre ellos HDLC y LAPB.

SDSL (*very-high-data-rate digital subscriber line*). Línea Digital del Subscriptor de altísima velocidad. Una de las cuatro tecnologías DSL. VDSL entrega entre 13 y 52 Mbps hacia abajo (desde la oficina central al lugar del cliente) y entre 1.5 y 2.3 hacia arriba (desde el lugar del cliente a la oficina central) sobre un único par de cobre trenzado. El funcionamiento de VDSL está limitado a un rango de entre 304,8 y 1.372 metros. Vea también DSL, ADSL, HDSL y VDSL.

Segmentación. Proceso de división de un solo dominio de colisión en dos o más dominios de colisión para reducir las colisiones y la congestión de la red.

Segmento. 1. Sección de una red que está rodeada de puentes, routers o switches. 2. En una LAN que usa topología de bus, un circuito eléctrico continuo que a menudo está conectado a otros segmentos similares a través de repetidores. 3. En la especificación TCP, una unidad única de información de capa de transporte. Los términos datagrama, trama, mensaje y paquete también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

Semidúplex. Capacidad de transmisión de datos en una sola dirección a la vez entre una estación transmisora y otra receptora. Comparar con full dúplex y unidireccional.

Señalización. En el contexto RDSI, el proceso de configuración de llamada utilizado, como establecimiento de la llamada, terminación de la llamada, información y mensajes varios, incluyendo configuración, conexión, liberación, información del usuario, cancelación, estado y desconexión.

Señalización de bit A&B. Procedimiento utilizado en las instalaciones de transmisión de T1, en el que cada uno de los 24 subcanales T1 dedica 1 bit de cada seis tramas a la información de señalización supervisora.

Servidor. Nodo o programa de software que suministra servicios a los clientes. Ver también cliente.

Servidor de empresa. Servidor que soporta a todos los usuarios en una red, ofreciendo servicios como correo electrónico o Sistema de Denominación de Dominio (DNS). Comparar con servidor de grupo de trabajo.

Servidor de grupo de trabajo. Servidor que soporta un conjunto específico de usuarios y ofrece servicios tales como procesamiento de texto y compartir archivos, que son servicios que solo algunos grupos de personas necesitan. Comparar con servidor de empresa.

Servidor de nombre. Servidor conectado a una red que resuelve nombres de red en direcciones de red.

Sesión. 1. Conjunto relacionado de transacciones de comunicaciones orientadas a conexión entre dos o más dispositivos de red. 2. En SNA, una conexión lógica que permite que dos unidades de red direccionables se comuniquen.

Sistema Básico de Entrada/Salida de Red. Ver NetBIOS.

SLIP (*Protocolo Internet de Enlace Serial*). Protocolo estándar para las conexiones seriales punto a punto que utiliza una variación de TCP/IP. El antecesor del PPP.

SMI (*Estructura de Administración de la Información*). Documento (RFC 1155) que especifica normas que se usan para definir objetos administrados en la MIB.

SNA (*Arquitectura de Sistemas de Red*). Arquitectura de red grande, compleja, con gran cantidad de funciones, desarrollada en 1970 por IBM. Similar en algunos aspectos al modelo de referencia OSI, pero con varias diferencias. SNA está compuesto esencialmente por siete capas. Ver capa de control de flujo de datos, capa de control de enlace de datos, capa de control de ruta, capa de control físico, capa de servicios de presentación, capa de servicios de transacción y capa de control de transmisión.

SNMP (*Protocolo simple de administración de redes*). Protocolo de administración de redes utilizado casi con exclusividad en redes TCP/IP. El SNMP brinda una forma de monitorear y controlar los

dispositivos de red y de administrar configuraciones, recolección de estadísticas, desempeño y seguridad.

Socket. 1. Estructura de software que funciona como un punto final de las comunicaciones dentro de un dispositivo de red (similar a un puerto). 2. Entidad direccionable dentro de un nodo conectado a una red AppleTalk; los sockets son propiedad de procesos de software denominados clientes de socket. Los sockets AppleTalk se dividen en dos grupos: las SAS, que están reservadas para clientes como, por ejemplo, los protocolos principales AppleTalk, y las DAS, que son asignadas de forma dinámica por DDP a pedido de los clientes del nodo. Un socket AppleTalk es conceptualmente similar a un puerto TCP/IP.

Software Cisco IOS (*Sistema Operativo de Internetwork*). Software de sistema de Cisco que proporciona funcionalidad, escalabilidad y seguridad comunes a todos los productos bajo la arquitectura CiscoFusion. El software Cisco IOS permite la instalación y administración centralizada, integrada y automatizada de internetwork, garantizando al mismo tiempo la compatibilidad con una amplia variedad de protocolos, medios, servicios y plataformas.

SOHO (*Oficina pequeña/oficina hogareña)*. Oficina pequeña u hogareña que incluye pocos usuarios que requieren una conexión que brinde conectividad más rápida y confiable que una conexión de marcado analógico.

SONET. Es una tecnología óptima para el tráfico de voz TDM, pero no puede escalar para hacer frente a las demandas exponenciales de ancho de banda ni puede entregar la flexibilidad multiservicio que necesitan las redes actuales.

Spanning Tree. Subconjunto sin bucles de una topología de red de capa 2 (conmutada).

SPID (*Identificador del perfil de servicio*). Número que algunos proveedores de servicios usan para definir los servicios a los cuales se suscribe un dispositivo RDSI. El dispositivo RDSI usa el SPID al acceder al switch que inicializa la conexión a un proveedor de servicio.

Split Horizon. Función destinada a evitar que los routers tomen rutas erróneas. El horizonte dividido evita que se produzcan bucles entre routers adyacentes y mantiene reducido el tamaño de los mensajes de actualización.

Spoofing. 1. Esquema que usan los routers para hacer que un host trate a una interfaz como si estuviera funcionando y soportando una sesión. El router hace spoofing de respuestas a mensajes de actividad del host para convencer a ese host de que la sesión continúa. El spoofing resulta útil en entornos de enrutamiento como DDR, en el cual un enlace de conmutación de circuito se desconecta cuando no existe tráfico que se deba enviar a través del enlace, a fin de ahorrar gastos por llamadas de pago. 2. La acción de un paquete que ilegalmente dice provenir de una dirección desde la cual en realidad no se lo ha enviado. El spoofing está diseñado para contrarrestar los mecanismos de seguridad de la red, tales como los filtros y las listas de acceso.

Spoofing de temporizador. Subconjunto de spoofing que se refiere específicamente al router que actúa especialmente para un cliente NetWare enviando paquetes de temporizador a un servidor NetWare para mantener activa la sesión entre el cliente y el servidor. Es de utilidad cuando el cliente y el servidor están separados por un enlace de WAN DDR.

SPP (*Protocolo de Paquete Secuenciado*). Protocolo que brinda transmisión de paquetes con control de flujo, basada en conexión a nombre de procesos del cliente. Parte del conjunto de protocolos XNS.

SPX (*Intercambio de Paquete Secuenciado*). Protocolo confiable, orientado a conexión, que complementa el servicio de datagramas suministrado por los protocolos de capa de red. Novell derivó este protocolo de transporte NetWare de uso común del SPP del conjunto de protocolos XNS.

SQE (*Error de calidad de señal*). En Ethernet, una transmisión enviada por un transceptor de vuelta al controlador para hacer saber al controlador si el circuito de colisión es funcional. También denominado heartbeat.

SS7 (*Sistema de Señalización Número 7*). Sistema de canal de señalización común desarrollado por Bellcore, utilizado en RDSI, que usa mensajes y señales de control telefónico entre los puntos de transferencia en el camino al destino llamado.

SSAP (*Punto de acceso al servicio origen*). SAP del nodo de red designado en el campo Origen de un paquete. Comparar con DSAP. Ver también SAP.

STP (*Par trenzado blindado*). Medio de cableado de dos pares que se usa en diversas implementaciones de red. El cableado STP posee una capa de aislamiento blindada para reducir la interferencia electromagnética. Comparar con UTP. Ver también par trenzado.

Subinterfaz. Una de una serie de interfaces virtuales en una sola interfaz física.

Subnetwork. Ver subred.

Subred. 1. Red segmentada en una serie de redes más pequeñas. 2. En redes IP, una red que comparte una dirección de subred individual. Las subredes son redes segmentadas de forma arbitraria por el administrador de la red para suministrar una estructura de enrutamiento jerárquica, de varios niveles mientras protege a la subred de la complejidad de direccionamiento de las redes conectadas. A veces se denomina subnetwork. 3. En redes OSI, un conjunto de sistemas finales y sistemas intermedios bajo el control de un dominio administrativo exclusivo y que utiliza un protocolo de acceso de red exclusivo.

SVC (*Circuito virtual conmutado*). Circuito virtual que se establece de forma dinámica a pedido y que se desconecta cuando la transmisión se completa. Los SVC se usan en situaciones en las que la transmisión de datos es esporádica. Comparar con PVC.

Switch. Dispositivo que conecta PC. El switch actúa de manera inteligente. Puede agregar ancho de banda, acelerar el tráfico de paquetes y reducir el tiempo de espera. Los switches son más "inteligentes" que los "hubs" y ofrecen un ancho de banda más dedicado para los usuarios o grupos de usuarios. Un switch envía los paquetes de datos solamente a la PC correspondiente, con base en la información que cada paquete contiene. Para aislar la transmisión de una PC a otra, los switches establecen una conexión temporal entre la fuente y el destino, y la conexión termina una vez que la conversación se termina.

Switch de LAN. Switch de alta velocidad que envía paquetes entre segmentos de enlace de datos. La mayoría de los switches de LAN envían tráfico basándose en las direcciones MAC. Los switches de LAN a menudo se clasifican según el método utilizado para enviar tráfico: conmutación de paquetes por método de corte o conmutación de paquetes por almacenamiento y envío. Un ejemplo de switch de LAN es el Cisco Catalyst 5000.

T:

T1. Servicio de portadora WAN digital que transmite datos formateados DS-1 a 1,544 Mbps a través de la red de conmutación telefónica, usando la codificación AMI o B8ZS. Comparar con E1.

T3. Servicio de portadora WAN digital que transmite datos formateados DS-3 a 44,736 Mbps a través de la red de conmutación telefónica. Comparar con E3.

TA (*Adaptador de terminal*). Dispositivo usado para conectar conexiones BRI de RDSI a interfaces existentes como EIA/TIA-232. Esencialmente es un módem RDSI.

Tabla de enrutamiento. Tabla almacenada en un router o en algún otro dispositivo de internetwork que realiza un seguimiento de las rutas hacia destinos de red específicos y, en algunos casos, las métricas asociadas con esas rutas.

TACACS (*Sistema de Control de Acceso al Controlador de Acceso a la Terminal*). Protocolo de autenticación, desarrollado por la comunidad DDN, que suministra autenticación de acceso remoto y servicios relacionados, como, por ejemplo, el registro de eventos. Las contraseñas de usuario se administran en una base de datos central en lugar de administrarse en routers individuales, suministrando una solución de seguridad de red fácilmente escalable.

Tamaño de ventana. Cantidad de mensajes que se pueden transmitir mientras se espera recibir un acuse de recibo.

Tarjeta de interfaz de red. Ver NIC.

TCP (*Protocolo de Control de Transmisión*). Protocolo de capa de transporte orientado a conexión que provee una transmisión confiable de datos de dúplex completo. TCP es parte de la pila de protocolo TCP/IP.

TCP/IP (*Protocolo de Control de Transmisión /Protocolo Internet*). Nombre común para el conjunto de protocolos desarrollados por el DoD de EE.UU. en los años 70 para promover el desarrollo de internetwork de redes a nivel mundial. TCP e IP son los dos protocolos más conocidos del conjunto.

TDM (*Multiplexado por división de tiempo*). Señal de conmutación de circuito utilizada para determinar la ruta de llamada, que es una ruta dedicada entre el emisor y el receptor.

TDM (*Multiplexión por División de Tiempo*). Técnica mediante la cual se puede asignar ancho de banda a la información procedente de múltiples canales en un solo cable, con base en espacios de tiempo asignados previamente. El ancho de banda se asigna a cada canal sin tomar en cuenta si la estación tiene datos para transmitir.

TE1 (*Equipo terminal tipo 1*). Dispositivo compatible con la red RDSI. TE1 se conecta a una terminación de red de Tipo 1 o Tipo 2.

TE2 (*Equipo terminal tipo 2*). Dispositivo no compatible con la red RDSI que requiere un adaptador de terminal.

Telnet. Protocolo de emulación de terminal estándar de la pila de protocolo TCP/IP. Telnet se usa para la conexión de terminales remotas, permitiendo que los usuarios se registren en sistemas remotos y utilicen los recursos como si estuvieran conectados a un sistema local. Telnet se define en RFC 854.

Temporizador maestro. 1. Mecanismo de hardware o software utilizado para disparar un evento o un escape de un proceso a menos que el temporizador se reajuste periódicamente. 2. En NetWare, un temporizador que indica el periodo máximo de tiempo durante el cual un servidor esperará que un cliente responda a un paquete de temporizador. Si el temporizador expira, el servidor envía otro paquete de temporizador (hasta una cantidad máxima establecida).

TFTP (*Protocolo de Transferencia de Archivos Trivial*). Versión simplificada de FTP que permite la transferencia de archivos de un PC a otro a través de una red.

TIA (*Asociación de la Industria de las Telecomunicaciones*). Organización que desarrolla estándares relacionados con las tecnologías de telecomunicaciones. En conjunto, TIA y EIA han formalizado estándares, como EIA/TIA-232, para las características eléctricas de la transmisión de datos.

Tictac. Retardo en un enlace de datos que utiliza tictacs de reloj de PC IBM (aproximadamente 55 milisegundos). Un tictac equivale a un segundo.

Tiempo de conexión de llamada. Tiempo requerido para establecer una llamada conmutada entre dispositivos DTE.

Tiempo de existencia. Ver TTL.

Token. Trama que contiene información de control. La posesión del token permite que un dispositivo de red transmita datos a la red.

Token Ring. LAN de transmisión de tokens desarrollada y soportada por IBM. Token Ring se ejecuta a 4 o 16 Mbps a través de una topología de anillo. Similar a IEEE 802.5.

TokenTalk. Producto de enlace de datos de Apple Computer que permite que una red AppleTalk se conecte mediante cables Token Ring.

Topología. Disposición física de los nodos y medios de red en una estructura de networking a nivel empresarial.

Topología de anillo. Topología de red compuesta por una serie de repetidores conectados entre sí por enlaces de transmisión unidireccionales para formar un bucle cerrado único. Cada estación de la red se conecta a la red a través de un repetidor. Aunque son anillos lógicos, las topologías de anillo a menudo se organizan en una estrella de bucle cerrado. Comparar con topología de bus, topología en estrella y topología en árbol.

Topología de bus. Topología de LAN en la que las transmisiones desde las estaciones de la red se propagan a lo largo del medio y son recibidas por todas las demás estaciones. Comparar con topología de anillo, topología en estrella y topología en árbol.

Topología de malla completa. Topología en la que todos los dispositivos Frame-Relay tienen un PVC hacia todos los demás dispositivos en una WAN multipunto.

Topología de malla parcial. Topología en la cual no todos los dispositivos en la nube Frame-Relay tienen un PVC hacia cada uno de los demás dispositivos.

Topología en árbol. Topología de LAN similar a una topología de bus, salvo que las redes en árbol pueden tener ramas con varios nodos. Las transmisiones desde una estación se propagan a lo largo del

medio y todas las demás estaciones las reciben. Comparar con topología de bus, topología de anillo y topología en estrella.

Topología en estrella. Topología de LAN en la que los puntos finales de una red se encuentran conectados a un switch central común mediante enlaces punto a punto Una topología de anillo que se organiza en forma de estrella implementa una estrella de bucle cerrado unidireccional, en lugar de enlaces punto a punto. Comparar con topología de bus, topología de anillo y topología en árbol.

Tormenta de broadcast. Suceso de red no deseado, en el que se envían varios broadcasts simultáneamente a todos los segmentos de red. Una tormenta de broadcast usa una parte considerable del ancho de banda de la red y normalmente hace que se agoten los tiempos de espera de la red. Ver también broadcast.

Traceroute. Programa disponible en varios sistemas que rastrea la ruta que recorre un paquete hacia un destino. Se utiliza a menudo para depurar los problemas de enrutamiento entre hosts. Existe también un protocolo traceroute definido en RFC 1393.

Trama. Agrupamiento lógico de información enviada como unidad de capa de enlace de datos a través de un medio de transmisión. A menudo se refiere al encabezado y a la información final, utilizadas para la sincronización y control de errores, que rodean los datos del usuario contenidos en la unidad. Los términos datagrama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

Transmisión de tokens. Método de acceso mediante el cual los dispositivos de red acceden al medio físico de forma ordenada basándose en la posesión de una pequeña trama denominada token. Comparar con switching y contención de circuitos.

Transmisión en paralelo. Método de transmisión de datos en el que los bits de un carácter de datos se transmiten de forma simultánea a través de una serie de canales. Comparar con transmisión serial.

Transmisión serial. Método de transmisión de datos en el cual los bits de un carácter de datos se transmiten de forma secuencial a través de un solo canal. Comparar con transmisión en paralelo.

TTL (*Tiempo de Existencia*). Campo en un encabezado IP que indica el tiempo durante el cual se considera válido un paquete.

Tunneling. Arquitectura diseñada para suministrar los servicios necesarios para implementar cualquier esquema de encapsulamiento punto a punto estándar.

U:

UDP (*Protocolo de Datagrama de Usuario*). Protocolo no orientado a conexión de la capa de transporte de la pila de protocolo TCP/IP. UDP es un protocolo simple que intercambia datagramas sin confirmación o garantía de entrega y que requiere que el procesamiento de errores y las retransmisiones sean manejados por otros protocolos. UDP se define en la RFC 768.

UNI (*Interfaz de Red a Usuario*). Especificación que define un estándar de interoperabilidad para la interfaz entre productos (un router o un switch) ubicados en una red privada y los switches ubicados dentro de las redes de carriers públicas. También utilizado para describir conexiones similares en redes Frame-Relay.

Unicast. Mensaje que se envía a un solo destino de red.

Unidireccional. Capacidad de transmisión en una sola dirección entre una estación emisora y una estación receptora. La televisión es un ejemplo de tecnología unidireccional. Comparar con full dúplex y semidúplex.

URL (*Localizador de recursos uniforme*). Esquema de direccionamiento estandarizado para acceder a documentos de hipertexto y otros servicios utilizando un explorador de Web.

UTP (*Par trenzado no blindado*). Medio de cable de cuatro pares que se emplea en varias redes. UTP no requiere el espacio fijo entre conexiones que es necesario para las conexiones de tipo coaxial. Hay cinco tipos de cableado UTP de uso común: cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3, cableado de Categoría 4 y cableado de Categoría 5. Comparar con STP.

V:

VCC (*Interconexión vertical*). Conexión utilizada para interconectar los diversos IDF al MDF central.

VDSL (*very-high-data-rate digital subscriber line*). Línea Digital del Subscriptor de altísima velocidad. Una de las cuatro tecnologías DSL. VDSL entrega entre 13 y 52 Mbps hacia abajo (desde la oficina central al lugar del cliente) y entre 1.5 y 2.3 hacia arriba (desde el lugar del cliente a la oficina central) sobre un único par de cobre trenzado. El funcionamiento de VDSL está limitado a un rango de entre 304,8 y 1.372 metros. Vea también DSL, ADSL, HDSL y SDSL.

Velocidad asegurada. Rendimiento de datos a largo plazo, en bits o celdas por segundo, que una red ATM puede proporcionar bajo condiciones normales de la red. La velocidad asegurada se encuentra asignada en un 100 por ciento. Se deduce en su totalidad del ancho de banda troncal a lo largo de la ruta del circuito. Comparar con velocidad excesiva y velocidad máxima.

Velocidad de acceso local. Velocidad de reloj (velocidad de puerto) de la conexión (bucle local) a la nube Frame-Relay. Es la velocidad a la que se desplazan los datos hacia o desde la red.

Velocidad excesiva. Tráfico que supera la velocidad asegurada de una conexión en particular. Específicamente, la velocidad excesiva es igual a la velocidad máxima menos la velocidad asegurada. El tráfico excesivo se entrega solamente si los recursos de red están disponibles y se pueden descartar durante los períodos de congestión. Comparar con velocidad asegurada y velocidad máxima.

Velocidad máxima. Rendimiento total máximo de datos que se permite en un circuito virtual determinado, que es igual a la suma del tráfico asegurado y del tráfico no asegurado desde el origen del tráfico. Los datos del tráfico no asegurado pueden descartarse si la red se congestiona. La velocidad máxima, que no puede superar la velocidad del medio, representa el rendimiento de datos más elevado que el circuito virtual puede enviar, medida en bits o en celdas por segundo. Comparar con velocidad excesiva y velocidad asegurada.

Ventana. Cantidad de octetos que el remitente desea aceptar.

Ventana deslizante. Ventana cuyo tamaño se negocia dinámicamente durante la sesión TCP.

VLAN (*LAN virtual*). Grupo de dispositivos de una LAN que están configurados (usando el software de administración) de tal modo que se pueden comunicar como si estuvieran conectados al mismo cable, cuando, en realidad, están ubicados en una serie de segmentos de LAN distintos. Debido a que

las LAN virtuales están basadas en conexiones lógicas en lugar de físicas, son extremadamente flexibles.

VLAN de puerto central. VLAN en la que todos los nodos en la misma VLAN se conectan al mismo puerto de switch.

VLAN dinámica. VLAN basada en las direcciones MAC, las direcciones lógicas o el tipo de protocolo de los paquetes de datos. Comparar con VLAN estática. Ver también LAN y VLAN.

VLAN estática. VLAN en la que los puertos de un switch se asignan estáticamente. Comparar con VLAN dinámica. Ver también LAN y VLAN.

VoIP (*Voice over IP*). La habilidad para transportar voz telefónica normal sobre una red de datos basada en el protocolo de Internet, con la misma funcionalidad, confiabilidad y calidad de voz que ofrecen las empresas telefónicas tradicionales. La Voz sobre protocolo Internet le permite a un router llevar tráfico de voz (por ejemplo llamadas telefónicas y faxes) sobre una red IP. En Voz sobre IP, la parte de dominio específica (DSP) segmenta la señal de voz en tramas, las cuales son luego agrupadas en parejas y guardadas en paquetes de voz. Estos paquetes de voz son transportados utilizando IP, de acuerdo con la especificación ITU-T H.323.

VPN (*Virtual Private Network*). Una Red Privada Virtual, permite establecer una conexión segura a través de una red pública o Internet. Una VPN permite que el tráfico IP viaje seguro a través de una red pública TCP/IP al encriptar el tráfico desde una red hasta la otra. Una VPN usa tunneling para encriptar toda la información en el nivel IP.

W:

WAN (*Red de área amplia*). Red de comunicación de datos que sirve a usuarios dentro de un área geográfica extensa y a menudo usa dispositivos de transmisión suministrados por carriers comunes. Frame-Relay, SMDS y X.25 son ejemplos de WAN. Comparar con LAN y MAN.

Wi-Fi (*Wireless-Fidelity*). Esta denominación, aplicada al protocolo inalámbrico IEEE 802.11b, significa que, vía radio, mantiene con fidelidad las características de un enlace Ethernet cableado.

Wi Max (*Worldwide Interoperability for Microwave Access*). Es la marca que certifica que un producto está conforme con los estándares de acceso inalámbrico "IEEE 802.16". Estos estándares permitirán conexiones de velocidades similares al ADSL o al cablemódem, sin cables, y hasta una distancia de 50-60 km. Este nuevo estándar será compatible con otros anteriores, como el de Wi-Fi (IEEE 802.11).

X:

X.25. Estándar UIT-T que define la manera en que las conexiones entre los DTE y DCE se mantienen para el acceso a la terminal remota y las comunicaciones en PC en las redes de datos públicas. Frame-Relay ha reemplazado en cierta medida a X.25.

XNS (*Sistema de red de Xerox*). Conjunto de protocolo originalmente diseñado por PARC. Muchas empresas de networking para PC tales como 3Com, Banyan, Novell y UB Networks utilizaron o actualmente utilizan una variante de XNS como protocolo de transporte primario.

ÍNDICE ALFABÉTICO

SÍMBOLOS

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z