UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES "ARAGON"

"IMPLEMENTACION DE PRÁCTICAS PARA EL ÁREA DE COMUNICACIONES BASADO EN LA CERTIFICACION CISCO CCNA"

T E S I S

QUE PARA OBTENER EL TITULO DE:

I N G E N I E R O M E C Á N I C O E L E C T R I C I S T A

P r e s e n t a :

MIGUEL ANGEL HERNÁNDEZ ORTÍZ

ASESOR:
ING. PRÓCORO PABLO LUNA ESCORZA

MARZO 2003.

Esta tesis la dedico toda mi familia, que siempre me apoyó en todo momento y supieron guiarme para lograr esta meta. A la Universidad Nacional Autónoma de México, que me brindó una segunda oportunidad, y a mis padres y hermana que es lo mas valioso que tengo, mis logros son los suyos.

Por mi Raza Hablará El Espíritu
Marzo de 2003

Presidente	Ing. Raúl Barrón Vera
Vocal	Ing. Narciso Acevedo Hernández
Secretario	Ing. Adrián Paredes Romero
Suplente	Ing. Prócoro Pablo Luna Escorza
Suplente	Ing. Javier Alain Morones Camacho

Índice

Capítulo 1 Introducción al sistema operativo

1.1. El IOS y su interfase de usuario 1
1.1.1. Componentes de los ruteadores 1
1.1.2. Línea de Comandos de la interfase (CLI) 2
1.1.3. Navegando en la línea de comandos de la interfase(CLI) del sistema operativo IOS 3
1.1.4. Syslog y Debug 5
1.2. Proceso de configuración y el Archivo de la Configuración 5
1.2.1. Manejando los Archivos de la Configuración 7
1.2.2. Protocolo Discovery de Cisco (CDP) 8
1.3. Modelo de referencia OSI y comunicación en capas 10
1.3.1. El modelo OSI origen y evolución 10
1.3.2. Capas de OSI 11
1.3.3. Los Beneficios del modelo en capas y Conceptos 13
1.3.4. La interacción Entre las Capas de OSI 14
1.3.5. Interacciones Entre las Capas Adyacentes en la Misma Computadora 14
1.3.6. Interacciones Entre las Mismas Capas en diferentes Computadoras 16
1.3.7. Encapsulamiento de datos 16
1.3.8. Los protocolos TCP/IP y NetWare 19
1.3.9. Funciones de la capa de Transporte de OSI 19
1.4. Funciones de la capa de enlace de Datos de OSI 20
1.5. Funciones de la capa de red de OSI 27
1.5.1. Ruteo 27
1.5.2. Un Comentario Sobre los Enlaces de Datos 28
1.5.3. Direccionamiento en la Capa de Red (Capa 3) 30
1.5.4. Ejemplo de capa 3 Estructuras de las Direcciones 31
1.5.5. Protocolos de ruteo 32
1.5.6. Protocolos No ruteables 32
1.6. Protocolos orientados a conexión Contra los no orientados a Conexión 32
1.6.1. Cómo se cumple la recuperación de Error 33
1.6.2. El control de flujo 35
1.6.3. Almacenamiento en el búfer (Buffering) 36
1.6.4. La Anulación de congestión 36
1.6.5. Ventaneo 37
1.6.6. Resumen de control de flujo 37

Capítulo 2 Redes Lan

2.1. Introducción 38
2.1.1. Switcheo LAN 38
2.1.2. Puenteo transparente 38
2.2. LANs Virtuales 38
2.2.1. Numerando los puertos (Interfaces) 39
2.2.2. Configuración Básica de IP y Puerto Dúplex 40

2.3. Protocolos de red 40
2.3.1. Protocolos TCP/IP 40
2.3.1.1. Protocolo de Control de Transmisión (TCP) 40
2.3.1.1.1. Transferencia de Datos Pedidos 41
2.3.1.1.2. Multiplexaje 41
2.3.1.1.3. Recuperación de Error (Fiabilidad) 41
2.3.1.1.4. Control de flujo Usando ventaneo 41
2.3.1.1.5. El Establecimiento de la Conexión y Terminación 41
2.3.1.2. Protocolo de Datagrama de Usuario (UDP) 41
2.3.1.3. Protocolo de resolución de dirección (ARP) 42
2.3.1.4. Protocolo de mensaje de control de Internet (ICMP) 42
2.3.1.5. FTP y TFTP 42
2.3.1.5.1. FTP 42
2.3.1.5.2. TFTP 43
2.4. Direccionamiento privado 43
2.4.1. Traducción de las direcciones de la red 43
2.4.2. Direccionamiento IPX y ruteo 44
2.5. Protocolos de Ruteo 45
2.5.1. Protocolos de Ruteo de Vector de Distancia 46
2.5.2. Comparando los Protocolos de Ruteo 46
2.5.3. Ruteo de vector de distancia 46
2.5.4. El Horizonte partido, Holddown, y Envenenamiento de la Ruta 47
2.5.5. RIP e IGRP 47
2.5.6. Resumen de los protocolos de ruteo de vector de distancia 47
2.6. Configuración de RIP e IGRP 47
2.6.1. El comando red (network) 48
2.6.2. Métrica IGRP 58
2.6.3. Rutas múltiples hacia la misma subred 49
2.7. Configurando el ruteo y mas protocolos de ruteo 49
2.7.1. IPX RIP, SAP, y GNS 49
2.7.2. Protocolo de Anuncio de Servicio 50
2.7.3. Entubado 50
2.8. Líneas Arrendadas punto a punto 51
2.8.1. Compresión 54
2.9. Protocolos Frame Relay 54
2.9.1. Características de Frame Relay y terminología 54
2.9.2. Direccionamiento DLCI y switchweo Frame Relay 56
2.9.3. La capa de la red tiene relación con Frame Relay 59
2.10. ISDN
2.10.1. Uso Típico 59
2.10.2. Multienlace PPP 61
2.10.3. Ruteo bajo demanda y configuración ISDN 62

Capitulo 3 Configuraciones y Simuladores

3.1. Introducción 65
3.2. Configuración básica del switch 1900 65

3.2.1. Configuración predefinida del switch 1900 65
3.3. Configuración básica de VLAN 67
3.3.1. Configuración de muestra para un Solo switch 68
3.4. Configuración IP 70
3.4.1. Direccionamiento IP con subinterfases Frame Relay 80
3.5. Configuración IPX 82
3.6. Configuración de RIP e IGRP 95
3.7. Configuración HDLC y PPP 96
3.8. Configuración Frame Relay 98
3.8.1. Configurando redes con subinterfases Punto a punto 99
3.8.2. Configurando redes con subinterfases coexistentes Punto a punto y Multipunto 102
3.9. Configuración ISDN 106
3.10. Simuladores 110
3.10.1. ¿Que son los simuladores? 110
3.10.2. Simuladores de ruteadores 111
3.11. Software Boson Router simulator 111
3.11.1. Características: 111
3.11.2. Requerimientos del sistema 112

Capítulo 4 Configuraciones de casos reales

4.1. Acceso al ruteador 113
4.1.1. Puerto de la consola 113
4.1.2. Puertos VTY 114
4.1.3. Añadir líneas de VTY 114
4.1.4. Puerto auxiliar 114
4.1.5. Puerto Telnet 114
4.2. Una configuración sencilla de Frame Relay 114
4.2.1. Red sencilla de voz sobre IP 115
4.2.2. Resumen de la red 115
4.2.3. Revisión de la configuración 118
4.3. Ruteador serie 2500 de Cisco 119
4.4. Switches 120
4.4.1. Descripción del sistema 121
4.5. Configuración Frame Relay real de un ruteador 122
4.6. Configuración de voz sobre Frame Relay 123

Capítulo 5 Prácticas

5.1. Estructura de las prácticas 127
5.1.1. Contenido de las prácticas 128
5.2. Prácticas para el laboratorio de comunicaciones 128
5.2.1. Práctica 1 Sistema Operativo de Cisco 139

5.2.2.	Práctica 2	Introducción al simulador	135
5.2.3.	Práctica 3	Introducción a redes LAN	140
5.2.4.	Práctica 4	Subnetting y Ruteo	145
5.2.5.	Práctica 5	Redes Lan Virtuales	153
5.2.6.	Práctica 6	Protocolo punto a punto	161
5.2.7.	Práctica 7	Frame Relay	168
5.2.8.	Práctica 8	ISDN	176

Conclusiones 178
Bibliografía 177

Introducción

¿Por que desarrollar este tema como tesis?

El interés de las empresas por conseguir una completa interconexión entre sus grandes corporativos y centros de distribución de bienes y/o servicios, para una mayor competitividad.
La continúa inundación por parte de los fabricantes de computadoras cada vez más potentes con dispositivos de comunicaciones.
Teléfonos celulares capaces de interactuar con dispositivos electrónicos de comunicación personales más avanzados y redes inalámbricas, o, simplemente la necesidad de contar con una conexión a Internet cada vez más eficiente, nos sugiere que debe haber un mayor crecimiento del personal capacitado para desarrollar, implementar y mantener tal tecnología para que soporte la carga de información que se requiere.
En los últimos años, la necesidad de una constante capacitación es determinante para competir adecuadamente en la industria de las telecomunicaciones, y se convierte en una necesidad para los recién egresados.
Y más aún cuando en otras instituciones como el tecnológico de Monterrey, campus estado de México o el tecnológico de Ecatepec, entre otras, ofrecen una educación orientada hacia la especialidad en interconexión de redes.
La meta de estas instituciones es que el alumno al completar sus estudios se encuentre lo suficientemente preparado como para inscribirse para el examen de certificación CCNA que ofrece Cisco y aprobarlo.
Por tal motivo los egresados de la Universidad Nacional Autónoma de México enfrentamos una desventaja.
Para contrarrestar este problema, esta tesis plantea una serie de prácticas para el laboratorio de comunicaciones, con esto se pretende complementar la formación de los estudiantes de esta carrera.

Debido a que el objetivo es implementar prácticas para el laboratorio de comunicaciones, esta tesis no abarcará los conceptos básicos, ya que en las materias teóricas correspondientes al área de comunicaciones se cubre satisfactoriamente con estos temas.

El objetivo es que el alumno comprenda el sistema operativo y logre configurar ruteadores de la marca Cisco, con la ayuda de simuladores y apegándose siempre al curso de certificación CCNA con el fin de lograr cierta habilidad y familiarizarse con este tipo de equipo y su funcionamiento además de reforzar los conocimientos teóricos, para que posteriormente se pueda aprobar el examen de certificación con mayor facilidad.

¿Quién es cisco Systems?

Cisco Systems es el líder mundial en redes para Internet. Las soluciones de conectividad de Cisco basadas en el protocolo de Internet (IP), son la base de Internet y de las redes corporativas, educativas y de gobierno en todo el mundo. Cisco entrega la línea más amplia de soluciones para el transporte de datos, voz y vídeo.

Cisco Systems es el líder mundial en redes para Internet. Las soluciones de Cisco conectan a la gente, las computadoras y las redes, permitiéndoles tener acceso o transmitir información sin importar las diferencias de tiempo, lugar o tipo de computadora.
Cisco ofrece soluciones de conectividad de extremo a extremo de la red, que los clientes utilizan para construir una infraestructura de información propia unificada o para conectarse a otra red. Una solución de conectividad de extremo a extremo es aquella que ofrece una arquitectura común

de servicios de red consistentes para todos los usuarios. Entre más amplio el rango de servicios de la red, mayor funcionalidad pueden obtener los usuarios conectados a ella.
Dentro de la industria, Cisco ofrece el rango más amplio de productos de hardware para conformar redes de información u ofrecer acceso a estas redes. Cisco ofrece también el software Cisco IOS, el cual entrega servicios de conectividad y permite a las aplicaciones trabajar en ambientes de red; experiencia y conocimiento en diseño e implantación de redes y soporte técnico y servicios profesionales para mantener y optimizar la operación de las redes. Cisco es único en su habilidad para ofrecer todos estos elementos, ya sea directamente o a través de sus socios de negocios.

Cisco sirve a sus clientes en tres grandes mercados:

- **Empresas.** Grandes organizaciones con necesidades complejas de conectividad, generalmente localizadas en múltiples lugares y con diferentes sistemas de cómputo. Entre los clientes empresariales se incluyen corporaciones, agencias gubernamentales e instituciones educativas y de servicios.
- **Proveedores de Servicio:** Compañías que ofrecen servicios de información, incluyendo empresas de telefonía, proveedores de servicio para Internet, compañías de cable y proveedores de comunicaciones inalámbricas.
- **Comercial:** Compañías o consumidores con necesidades de redes de datos, así como requerimientos para conectividad con sus socios de negocios o con Internet.

Cisco vende sus productos en aproximadamente 115 países a través de una fuerza directa de ventas, distribuidores, resellers de valor agregado e integradores de sistemas. Las oficinas principales de Cisco se encuentran en San José de California. También opera en Research Triangle Park, NC, y Chelmsford, MA, así como en más de 430 oficinas de soporte y venta en 60 países.

Certificación CCNA de Cisco

La certificación CCNA acredita las aptitudes de una persona para realizar trabajos en la red a un nivel básico. Los candidatos que aprueben los exámenes recibirán la certificación CCNA concedida por Cisco y pueden utilizar la designación de CCNA en sus tarjetas de negocios.

La certificación CCNA se otorga en dos temas:

- Enrutamiento y conmutación.
- Conmutación WAN.

Para ayudar a los candidatos a preparar los exámenes de certificación, los socios de formación Cisco ofrecen los siguientes servicios:

- Cursos presenciales y de aprendizaje electrónico
- Supervisión y salas de chat en línea
- Desarrollo de la formación práctica a través de laboratorios remotos a través de Internet.

El programa Cisco Networking Academy también ofrece preparación de CCNA para alumnos de institutos y universidades. Los materiales de formación a distancia pueden solicitarse a Cisco Learning Store.

Ventajas que ofrece la certificación

En general, la certificación de Cisco acredita el conocimiento personal, de manera que aumenta la credibilidad profesional de su titular y garantiza un alto nivel de conocimientos técnicos.
En particular, la certificación CCNA indica un conocimiento de redes del mercado SOHO y la capacidad para trabajar en empresas u organizaciones pequeñas cuyas redes tengan menos de cien nodos.
Un titular de CCNA puede hacer lo siguiente:

- Instalar y configurar switches y ruteadores de Cisco en redes con varios protocolos que utilicen interfaces LAN y WAN.
- Ofrecer un servicio de resolución de problemas de nivel 1.
- Mejorar el rendimiento y la seguridad de la red.

Los puestos a los que puede aspirar un titular de CCNA incluyen:

- Ingeniero de centros de asistencia técnica.
- Técnico de campo.
- Ingeniero de sistemas de nivel 1.
- Integrador de sistemas de nivel 1.

Requerimientos para ser parte del programa "Cisco Networking Academy"

El programa "Cisco Networking Academy" enseña a estudiantes las habilidades que necesitan para diseñar, instalar y mantener redes de información. Una Academia Local es una institución educativa que enseña el curriculum del programa a estudiantes.

Una Academia Local:

- Debe obtener y mantener correo electrónico activo y al menos una conexión dedicada a Internet igual a 64 Kbps (DS0).
- Debe contar con dos profesores que enseñen los cuatro módulos del curriculum. Estos profesores deben prepararse para obtener la certificación CCAI (Cisco Certified Academic Instructor).
- No debe tener más de tres alumnos por computadora (idealmente un alumno por computadora) en clase. Estas computadoras al menos deben cumplir con los siguientes requisitos:

Para PC:

Windows 95
Netscape 3.0 o posterior o Internet Explorer 4.0 o posterior
Java Script, QuickTime plug-in y MacroMedia Shockwave plug-in
(Estas aplicaciones están disponibles de manera gratuita en el Web).
Mínimo 486 con 24 MB en RAM
10 MB de espacio libre en disco
Resolución mínima del monitor de 800 x 600 con 256 colores.
Tarjeta de Red Ethernet 10BaseT
Drive para CD/ROM
Mouse
Tarjeta de Sonido
Audífonos o bocinas.

- Contar con cinco PCs o Macintosh para el desarrollo del laboratorio con las siguientes características:
  Windows 95 o Mac OS 7.5 o posterior
  Software de Emulación de terminal
  Tarjeta de Red Ethernet 10BaseT
  Netscape 3.0 o posterior o Internet Explorer 4.0 o posterior
  Puerto serial disponible
- Comprar el equipo de laboratorio para el programa de "Cisco Networking Academy". Este equipo consta de 5 ruteadores y 2 LAN Switches.
- Contar con cuatro hubs adicionales para el laboratorio (no incluidos).
- Contar con el resto de los materiales requeridos para el desarrollo del curriculum del programa (Ejemplo: herramientas, cableado, conectores RJ45, transceivers, equipos de medición de cables, odómetro).
- Adquirir el contrato de soporte denominado SMARTnet para el equipo de laboratorio una vez transcurrido el primer año (el primer año viene incluido con la compra del equipo).
- La Academia Local debe cumplir con las cuotas designadas por la Academia Regional por concepto del entrenamiento y soporte técnico, operativo y administrativo recibido por parte de la Academia Regional.
- Responder y enviar a la Academia Regional todos los reportes que éste pida sobre el desarrollo del programa

Capítulo 1 Introducción al sistema operativo

1.1. El IOS y su interfase de usuario

IOS, es una marca registrada de Cisco Systems, y es el nombre del sistema operativo que se encuentra en la mayoría de los ruteadores Cisco, dentro de los cuales corre el sistema operativo con su familiar de línea de comandos de la interfase (CLI – Command Line Interface)

1.1.1. Componentes de los ruteadores

Además de manejar la lógica de los paquetes de ruteo, el sistema operativo controla el uso de los diferentes componentes físicos, que incluyen la memoria, el procesador y las interfaces.
Todos los ruteadores Cisco tienen un puerto de consola y la mayoría tiene un puerto auxiliar pensado para el acceso administrativo local desde una terminal ASCII o una Computadora, usando un emulador de terminal. El puerto auxiliar, no encontrado en unos cuantos modelos de ruteadores Cisco, está pensado para el acceso dial asíncrono desde una terminal ASCII o un emulador de terminal.

Cada ruteador tiene diferentes tipos de memoria

- RAM – algunas veces llamada DRAM por Random Access Memory Dinámica, la memoria RAM es usada por el ruteador, así como se usa por cualquier otra computadora, para el almacenamiento mientras se esta trabajando.
- ROM - este tipo de memoria (Read Only Memory), guarda una imagen reiniciable del sistema operativo, la cual no es usada típicamente para operación normal. La memoria ROM contiene el código que es usado cuando el ruteador se inicializa, hasta cuando el ruteador sabe de donde obtener la imagen completa del sistema operativo
- Memoria Flash - La memoria Flash guarda una imagen del sistema operativo totalmente funcional y es la que el ruteador va a tomar al momento de inicializarse. La memoria flash también puede ser utilizada para guardar archivos de configuración en la serie 7500 de Cisco.
- NVRAM – La RAM No volátil. Guarda el archivo de configuración de inicio

Todos estos tipos de memoria son permanentes, excepto la memoria RAM. De tal modo que en los ruteadores Cisco no se encuentran discos duros o unidades de disquete para el almacenaje.

Los procesadores en los ruteadores varían de modelo en modelo. En la mayoría de los ruteadores, sólo está disponible una opción para el procesador; ya que, no es común que alguien pida un tipo del procesador específico o tarjeta. La excepción a esto son las familias 7200 y 7500 de ruteadores. Por ejemplo, en la serie 7500, Es posible escoger cualquier switch de ruteo con el Procesador 1 (RSP-1), RSP-2, o RSP-4. En cualquier caso, todos los ruteadores 7200 y 7500, así como la mayoría de las otras familias de ruteadores Cisco, ejecutan el IOS. Esta similitud le permite a Cisco que formule los exámenes, como el CCNA que cubra las características del IOS sin tener que tomar en cuentamuchos detalles del hardware.

Las interfaces son usadas por un ruteador para enrutar los paquetes y puentear las tramas a través de un ruteador. Los tipos de interfaces disponibles cambian con el tiempo debido a la nueva tecnología. Por ejemplo, paquete-sobre-SONET (packet over SONET) e interfaces de voz son relativamente recientes incorporaciones a la línea de productos. Sin embargo, existe un poco de confusión sobre cómo llamar a las tarjetas actuales que alojan las interfaces físicas.

Las interfaces físicas son denominadas como interfaces por los comandos del sistema operativo, en vez de llamarlos puertos o ranuras Si se esta familiarizado con los comandos del IOS en una

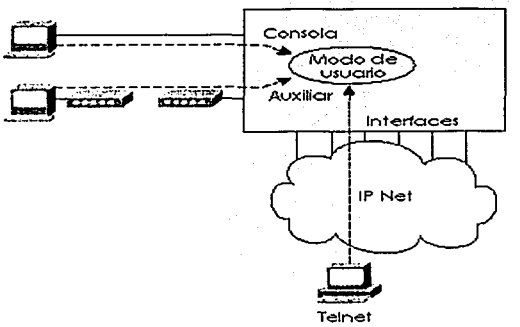
plataforma, entonces se estará familiarizado en otra. En algunos ruteadores más pequeños, el número de la interfase es un solo número. Sin embargo, con algunas otras familias de ruteadores, la interfase se numera primero con la ranura en que la tarjeta reside, seguido por una diagonal y después el número del puerto en esa tarjeta. Por ejemplo, el puerto 3 en la tarjeta, en la ranura 2, sería internase 2/3. Numerando las salidas con 0 para las ranuras de la tarjeta y 0 para los puertos en cualquier tarjeta. En algunos casos, la interfase se define por tres números: primero la ranura de la tarjeta, y la tarjeta auxiliar (típicamente llamada adaptador de puerto), y después, un número para la interfase física en el adaptador del puerto. Las familias 2600 y 3600 también usan un slot/port (ranura/puerto).

1.1.2. Línea de Comandos de la interfase (CLI)

Cisco acostumbra usar la sigla CLI (Command Line Interface) para referirse a la línea de comandos de la interfase de la terminal de usuario del sistema operativo IOS. El término CLI implica que el usuario teclee los comandos en una terminal, emulador de terminal, o conexión de Telnet.

Para acceder al CLI, se usa uno de los tres métodos ilustrados en Figura 2.

Figura 1 Acceso CLI



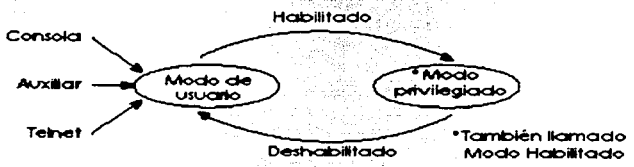
Sin tener en cuenta que método de acceso se usa, el usuario de CLI es situado en el modo de usuario o modo EXEC de usuario. EXEC se refiere al hecho en que los comandos que son tecleados en este modo son ejecutados, y algunos mensajes de respuesta son desplegados en pantalla.
Puede ser requerida una contraseña cuando se ingresa la ruteador, de hecho la configuración predeterminada del sistema operativo (IOS) 12.X requiere de una contraseña para el acceso por telnet y por el puerto auxiliar, aunque no se establezca ninguna contraseña, por lo que, se debe configurar primero las contraseñas de la consola. La tabla 1 muestra los diferentes tipos de contraseñas y la configuración para cada tipo.

Tabla1

Acceso desde...	Tipo de contraseña	Configuración
Consola	Contraseña de consola	**Line console** *0* **Login** **Password** *faith*
Auxiliar	Contraseña auxiliar	**Line aux** *0* **Login** **Password** *hope*
Telnet	Contraseña vty	**Line vty** *0 4* **Login** **Password** *love*

El comando **login** le indica al ruteador que despliegue el indicador. El comando **password** especifica la contraseña del texto a ser tecleada por el usuario para tener acceso. Se permiten varias conexiones de Telnet coexistentes a un ruteador. El comando **line vty** 04
Significa que esta configuración aplica a los vtys (virtual teletypes—terminals) de 0 hasta 4. Estos cinco vtys se permiten por el sistema operativo IOS, a menos que sea un IOS para un servidor de acceso de marcado o discado,
Estos cinco vtys, típicamente tienen la misma contraseña, lo que es de gran ayuda, ya que los usuarios que se conectan al ruteador vía Telnet no pueden escoger cual de los vty es designado a los usuarios.
El modo usuario EXEC, es uno de los dos modos en la interfase de usuario del sistema operativo. El modo "Enable" (también conocido como modo privilegiado o modo privilegiado EXEC) es el otro. El modo Enable se nombra así, debido al comando utilizado para alcanzar este modo, como se muestra en la figura 2.

Figura 2 Modos de usuario y privilegiado



1.1.3. Navegando en la línea de comandos de la interfase(CLI) del sistema operativo IOS

En la tabla 2, "Command" representa cualquier comando, no la palabra "command". Así como "parm" representa los parámetros del comando, no la palabra parámetro.

Cuándo se teclea "**?**", la línea de comandos de la interfase (Command Line Interface – CLI) reacciona inmediatamente; es decir, no se necesita presionar la tecla "Enter" o cualquier otra tecla. El ruteador también vuelve a mostrar en la pantalla lo que se tecleó antes de el comando "**?**". Si se presiona "Enter" inmediatamente después de "**?**", el IOS intenta ejecutar el comando con sólo los parámetros que se han tecleado ese momento.

El contexto en que la ayuda se pide también es importante. Por ejemplo, cuándo se teclea "**?**" en el modo usuario, no se despliegan todos los comandos, solo son desplegados en pantalla los comandos permitidos en el modo EXEC no privilegiado. La ayuda también está disponible en el modo de configuración; se despliegan sólo los comandos de la configuración en ese modo de funcionamiento.

Tabla 2

Tecleando	**La ayuda que se obtiene**
?	Ayuda para todos los comandos disponibles en este modo
Help	Texto que describe cómo conseguir la ayuda, no se da ayuda acerca de comandos
Command ?	Texto de ayuda que describe todas las primeras opciones del parámetro para el comando **command.**
Com?	Una lista de comandos que comienzan con "com"
Command parm?	Este tipo de ayuda estan todos los parámetros comenzando con "parm". Nótese que no hay espacio entre "parm" y "?"
Command parm<Tab>	Si el usuario aprieta la tecla Tab, el CLI deletreará el resto de este parámetro a la línea del comando para el usuario, o no hará nada. Si el CLI no hace nada, significa que esta serie de caracteres representa más de un posible parámetro siguiente, así que el CLI no sabe qué comando deletrear
Command parm1 ?	Si un espacio se inserta antes del signo de interrogación, el CLI lista todos los próximos parámetros y da una explicación breve de cada uno

Tabla 3

Comandos del teclado	**Lo que obtiene el usuario**
Flecha arriba o Ctrl + p	Esto despliega el comando recientemente usado. Si presiona de nuevo, el próximo comando más reciente aparece, hasta que el historial se agote. La p es la abreviatura de previous(previo)
Flecha abajo o Ctrl + n	Si se ha ido demasiado lejos regresando en la memoria del historial, estas teclas irán adelante, en orden de los comandos recientemente tecleados. La n es la abreviatura para next (siguiente)
Flecha izquierda o Ctrl + b	Esto mueve el cursor hacia atrás en el comando actualmente desplegado sin anular los caracteres. (La b es la abreviatura de back (atrás)
Flecha derecha o Ctrl + f	Mueve el cursor hacia adelante en el comando actual desplegado sin anular los caracteres. La f es la abreviatura de forward (Adelante)
Atrás	Esto mueve el cursor hacia atrás en el comando actualmente desplegado, mientras de borran los caracteres.
Ctrl + a	Esto mueve el cursor directamente al primer carácter del comando actualmente desplegado.
Ctrl + e	Esto mueve el cursor directamente al final del comando actualmente desplegado.
Esc + b	Esto mueve el cursor atrás una palabra en el comando actualmente desplegado.
Esc + f	Esto mueve el cursor la una palabra adelante en el comando actualmente desplegado.
Ctl + r	Esto crea un nuevo indicador para el comando, seguido por todos los caracteres tecleados desde que el último indicador del comando fue escrito. Esto es particularmente útil si los mensajes del sistema confunden la pantalla y es incierto lo que el usuario ha tecleado hasta ahora.

Los comandos que se usan, se guardan en el historial, el cual retiene los últimos 10 comandos que se teclearon. Se puede cambiar el tamaño del historial con el comando **terminal history size** x, donde x es el número de comandos que se guardan, y puede ajustarse a un valor entre 0 y 256.
Los comandos que se han utilizado previamente pueden recuperarse durante la actual conexión consola/aux/Telnet, para que después puedan editarse con el propósito de ahorrar tiempo. Esto es particularmente útil cuando se están tecleando largos comandos de configuración. La tabla 4 muestra los comandos usados para manipular comandos previamente usados.

1.1.4. Syslog y Debug

El Sistema operativo IOS crea mensajes cuando ocurren diferentes eventos y son enviados predeterminadamente por la consola. Estos mensajes se llaman mensajes syslog. El comando **debug** es una de las herramientas de diagnostico más importantes para solucionar problemas difíciles en un ruteador. El **debug** habilita el monitoreo de los puntos en el IOS y genera mensajes que describen lo que el IOS esta haciendo y viendo. Cuando se habilita cualquier opción del comando **debug**, el ruteador procesa los mensajes con la misma lógica como otros mensajes **syslog**.

Nota: El comando **no debug all** desactiva todos los **debug**. Antes de habilitar una opción poco familiar del comando **debug**, emitir un **no debug all** y después emitir el comando **debug** que se quiera usar; entonces, rápidamente recuperar el comando **no debug all**. Si los mensajes son voluminosos, de debe presionar Enter inmediatamente para intentar prevenir que el ruteador se congele, desactivando inmediatamente todos los **debug**.

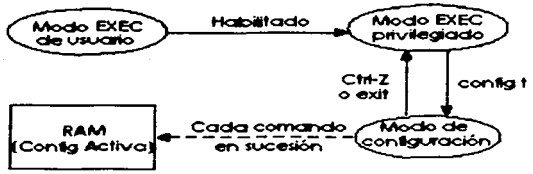
Los usuarios pueden o no estar interesados en ver los mensajes cuando aparecen. El puerto de la consola siempre recibe los mensajes syslog. Cuando un usuario emite un telnet al ruteador, no se ve ningún mensaje syslog a menos que el usuario emita el comando **terminal moitor**.
Este comando significa que simplemente esta terminal está supervisando los mensajes syslog. Otra alternativa para ver los mensajes syslog es tener los mensajes del IOS syslog grabados en el búfer de la memoria RAM, y entonces, usar el comando **show logging** para desplegar los mensajes. Para los usuarios de Telnet, tener los mensajes guardados en el búfer, usando el comando de configuración global **logging buffered** es particularmente útil, Porque los usuarios de Telnet no obtienen predeterminadamente los mensajes del syslog, sin embargo, estos usuarios pueden esperar y ver aparecer los mensajes cuando se desee. Finalmente, el subcomando de configuración de línea **logging synchronous** puede ser usado para la consola y los vtys para decirle al ruteador que espere hasta que el último comando que el usuario emita sea desplegado antes de mostrar cualquier mensaje del syslog en la pantalla. Eso proporciona un poco menos de interrupción para el usuario.
También pueden enviarse los mensajes de Syslog a otro dispositivo.

1.2. Proceso de configuración y el Archivo de la Configuración

El propósito del modo de configuración es cambiar la configuración del ruteador tecleando varios comandos de configuración. La figura 3 ilustra las relaciones entre el modo de configuración, modo de usuario EXEC, y modo privilegiado EXEC.

Los comandos tecleados en el modo de configuración, actualizan el archivo de configuración activa. Los cambios son movidos hacia el archivo de configuración activa, cada vez que el usuario presiona la tecla Enter, se tiene una respuesta inmediatamente del ruteador.
En el modo de configuración, los comandos context-setting (contexto de configuración) se usan antes de la mayoría de los comandos de configuración, por ejemplo si se está usando comandos de la interfase o de configuración. Estos comandos context-setting, le dicen al ruteador el tema sobre el cual se teclearán los comandos. Estos comandos le dicen al ruteador qué comandos listar cuando se pide la ayuda. Después de todo, el objetivo de estos contextos, es hacer la ayuda en línea más conveniente y clara.

Figura 3 Modo de configuración CLI contra el modo EXEC



El comando **interface** es el comando de configuración context-setting más comúnmente usado. Como un ejemplo, el usuario del CLI podría entrar en el modo de configuración de interfase después de teclear el comando de configuración **interface Ethernet 0**. El comando **help** en el modo de configuración Ethernet, despliega sólo comandos que son útiles al configurar las interfaces Ethernet. Los comandos usados en este contexto se llaman subcomandos, o, en este caso especifico, subcomandos de la interfase. La Figura 4 muestra varios contextos de modo de configuración diferentes, incluyendo el modo de configuración de interfase, e ilustra las relaciones y métodos de mover entre ellos.

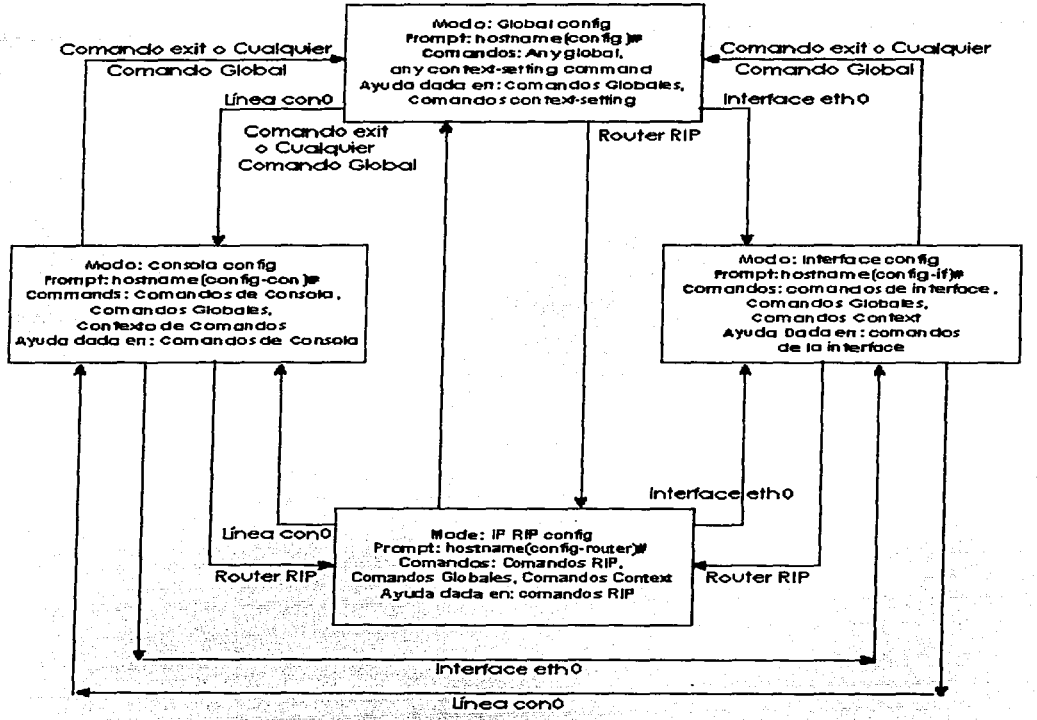
Las etiquetas en las líneas en Figura 4 representan la acción o comando que mueven al usuario un modo a otro. Por ejemplo, del modo de configuración de consola (el cuadro de la izquierda), el comando **interface ethernet 0** podría moverlo al cuadro de la derecha que representa el modo de configuración de la interfase.

No existe ninguna regla fija para saber cuales comandos son globales o subcomandos, pero generalmente, cuando pueden ponerse casos múltiples de un parámetro en un solo ruteador, el comando usado para establecer los parámetros, es probable que sea un subcomando de configuración.

Por ejemplo, el comando **hostname** es un comando global porque hay sólo un hostname por ruteador. El comando **interface ethernet 0** es un comando de configuración global, porque sólo hay una interfase en ese ruteador. Finalmente, el comando **ip address** es un subcomando de interfase que establece la dirección IP en la interfase; cada interfase tendrá una dirección IP diferente.

Use **Ctrl+z** desde cualquier parte del modo de configuración (o usar el comando **exit** del modo de configuración global) para salir del modo de configuración y volver al modo privilegiado EXEC. En el modo de configuración, el comando **end** también existe desde cualquier punto en el modo de configuración, regresando al modo privilegiado EXEC. El comando **end** en submodos o modos de configuración de contextos regresa un nivel hacia el modo global de configuración.

Figura 4



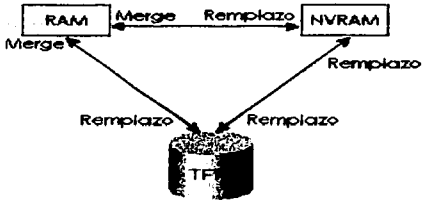
1.2.1. Manejando los Archivos de la Configuración

El archivo de configuración de inicio está en la memoria NVRAM; el otro archivo que está en la RAM es el que el ruteador usa durante el funcionamiento. El ruteador copia el archivo de configuración guardado en la NVRAM en la memoria RAM, como parte del proceso de arranque. Los archivos de configuración pueden guardarse remotamente como texto en código ASCII usando TFTP desde cualquier parte.

El método básico para manipular los archivos de configuración y moverlos dentro y fuera del ruteador, es usando un servidor TFTP. El comando "copiar" **copy** se usa para mover el archivo de

configuración entre la RAM, NVRAM, y un servidor TFTP. Los archivos pueden copiarse entre cualquier par, como lo muestra la Figura 5.

Figura 5 Localidades para copiar y resultados de las operaciones copiar



1.2.2. Protocolo Discovery de Cisco (CDP)

El Protocolo Discovery de Cisco (CDP) se usa por los ruteadores y switches de Cisco para determinar la información básica sobre los ruteadores y switches vecinos. Se puede usar esta información para aprender las direcciones rápidamente para un más fácil manejo del Protocolo de Dirección de Red Simple (SNMP), así como aprender las direcciones de otros dispositivos cuando no se tienen las contraseñas para ingresar en otro dispositivo.

Ejemplo 1 Opciones del comando show CDP

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

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
fred               Ser 1           172          R          2500      Ser 1
Yosemite           Ser 0.2         161          R          2500      Ser 0.2

Seville#show cdp entry fred
-------------------------
Device ID: fred
Entry address(es):
  IP address: 183.6.8.3
Platform: cisco 2500,  Capabilities: Router
Interface: Serial1,  Port ID (outgoing port): Serial1
Holdtime : 168 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(6), RELEASE SOFTWARE (fc1)
Copyright  1986-1999 by cisco Systems, Inc.
Compiled Tue 10-Aug-99 23:52 by phanguye

Seville#show cdp neighbor detail
-------------------------
Device ID: fred
Entry address(es):
```

```
  IP address: 163.5.8.3
Platform: cisco 2500,  Capabilities: Router
Interface: Serial1,  Port ID (outgoing port): Serial1
Holdtime : 164 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(6), RELEASE SOFTWARE (fc1)
Copyright  1986-1999 by cisco Systems, Inc.
Compiled Tue 10-Aug-99 23:52 by phanguye

-------------------------
Device ID: Yosemite
Entry address(es):
  IP address: 10.1.5.252
  Novell address: 5.0200.bbbb.bbbb
Platform: cisco 2500,  Capabilities: Router
Interface: Serial0.2,  Port ID (outgoing port): Serial0.2
Holdtime : 146 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(6), RELEASE SOFTWARE (fc1)
Copyright  1986-1999 by cisco Systems, Inc.
Compiled Tue 10-Aug-99 23:52 by phanguye

Seville#show cdp interface
Ethernet0 is up, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial0.2 is up, line protocol is up
  Encapsulation FRAME-RELAY
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial1 is up, line protocol is up
  Encapsulation HDLC
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds

Seville#show cdp traffic
CDP counters :
    Packets output: 41, Input: 21
    Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
    No memory: 0, Invalid packet: 0, Fragmented: 0
```

CDP es un protocolo propiedad de Cisco; para apoyar el envío de los mensajes del CDP sobre una interfase, esa interfase debe soportar las cabeceras SNAP. Cualquier interfase LAN, HDLC, Frame Relay, y ATM soporta el protocolo CDP. El ruteador o switch puede descubrir la Capa 3 direccionando los detalles de ruteadores vecinos, inclusive sin configurar ese protocolo de la capa 3, ya que CDP no depende de ningún protocolo de la capa 3 en particular.
CDP descubre varios detalles útiles del dispositivo vecino:

- Identificador del dispositivo - Típicamente el hostname.
- Lista de direcciones – Red y direcciones de enlace de datos
- Identificador del puerto - Texto que identifica el puerto que es otro nombre para una interfase.
- Lista de capacidades - información de lo que hace el dispositivo, en este caso un ruteador o un switch.
- Plataforma - El modelo y el sistema operativo que opera en el dispositivo

El CDP se habilita predeterminadamente en la configuración. El comando global **no cdp run** deshabilita CDP para todo el dispositivo, y el comando global **cdp run** re-habilita CDP. Igualmente, el subcomando de interfase **no cdp enable** desactiva el CDP sólo en esa interfase, y el comando de switches **cdp enable** regresa al estado predefinido de CDP que se habilita.

Una variedad está disponible de la opción del comando **show cdp**. El ejemplo lista el rendimiento de los comandos, seguido de algún comentario.

Los comandos proporcionan la información sobre los vecinos y el comportamiento del mismo protocolo CDP. En el ejemplo 4 el comando **show cdp entry** *fred*, se muestran todos los detalles aprendidos por el CDP y se resaltan en negritas. Para saber que fred es el identificador del dispositivo de un vecino, el comando **show cdp neighbor** puede usarse para resumir la información sobre cada vecino. **Show cdp neighbor detail** hace una lista de los detalles de todos los vecinos, en el mismo formato como **show cdp entry**. Además, **show cdp traffic**, hace una lista de arriba que el CDP introduce para realizar sus funciones.

1.3. Modelo de referencia OSI y comunicación en capas

En los años anteriores, la necesidad de entender el modelo de referencia de los Sistemas Abiertos de interconexión (OSI) creció rápidamente. El gobierno estadounidense aprobó leyes que les exigían a los distribuidores que apoyaran el software de OSI en sus sistemas, o el gobierno ya no compraría los sistemas. Varios distribuidores inclusive predijeron que el Internet global evolucionaría hasta usar los protocolos de OSI en lugar de TCP/IP. Sin embargo, OSI se ha ido implementado a una escala mucho menor de la que se había predicho.

Unos cuantos distribuidores impulsaron sus soluciones de software de OSI. Sin embargo, varios componentes del modelo OSI son implementados con popularidad hoy. Por ejemplo, las direcciones de la capa de red del Punto de Acceso de Servicio de Red (Network Service Access Point - SNAP) se usan a menudo para la señalización en el Modo del Transferencia Asíncrono (ATM) en las redes. Sin embargo, las implementaciones de las siete capas de OSI son relativamente raras hoy.

1.3.1. El modelo OSI origen y evolución

La dificultad en estos días cuando se usa las especificaciones del protocolo de OSI, como un punto de referencia es que casi nadie usa esas especificaciones. En una sala de cómputo no se podría ver, en cual de todas esas computadoras su principal, o incluso opcional, protocolo de ruteo esta definido por OSI.

OSI es el modelo de referencia del Sistema de Interconexión Abierto para las comunicaciones. OSI es un conjunto bien definido de especificaciones protocolares con muchas opciones para lograr las tareas similares. Algunos participantes en la creación y desarrollo del modelo OSI, quisieron que se convirtiera en el protocolo de red usado para todas las aplicaciones. El gobierno Estadounidense fue mas lejos, al requerir que OSI los apoya en cada computadora que compraran (a partir de cierta fecha a principios de 1990) vía un decreto llamado el perfil gubernamental OSI (GOSIP - government OSI Profile), qué ciertamente les dio algún incentivo a distribuidores para escribir el código de OSI.

1.3.2. Capas de OSI

El modelo de OSI consiste en siete capas, cada una de las cuales pueden tener varias subcapas. Las capas superiores del modelo OSI (aplicación, presentación, y sesión, capas 7, 6, y 5) se orientan más hacia los servicios de las aplicaciones. Las cuatro capas más bajas (transporte, red, enlace de datos, y física, capas 4, 3, 2, y 1) se orientan más hacia el flujo de datos de extremo a extremo a través de la red. Se trabajará principalmente con los problemas en las capas más bajas, en particular con la Capa 2 en donde se lleva a cabo la conmutación, y la Capa 3, donde el ruteo se lleva a cabo. La tabla 4 muestra los diagramas de las siete capas del modelo de referencia OSI con una descripción completa y una lista de protocolos de ejemplo.

Tabla 4

Nombre de la Capa	Descripción Funcional	Ejemplos
Aplicación (capa 7)	Una aplicación que comunica con otras computadoras esta implementada en los conceptos de la capa de aplicación de OSI. La capa de la aplicación se refiere a los servicios de comunicaciones hacia las aplicaciones. Por ejemplo, un procesador de texto que le falta las capacidades de comunicaciones no llevaría a cabo el código para las comunicaciones, y los programadores del procesador de texto no estarían involucrados en la capa 7 de OSI. Sin embargo, si fue agregada una opción para transferir un archivo, entonces el procesador de textos necesitaría implementar la capa 7 de OSI(o la capa equivalente en otra especificación protocolar).	Telnet, HTTP, FTP, WWW browsers, NFS, SMTP gateways (Eudora, CC:mail), SNMP, X.400 mail, FTAM
Presentación (capa 6)	El propósito principal de esta capa está en definir el formato de los datos, como el texto ASCII, texto de EBCDIC, binario, BCD, y JPEG. La encriptación también se define por OSI como un servicio de capa de presentación. Por ejemplo, FTP le permite escoger el traslado entre binario o ASCII. Si el binario se selecciona, el remitente y receptor no modifican los volúmenes del archivo. Si es escogido ASCII, el remitente traduce el texto del carácter del remitente puesto a un ASCII estándar y envía los datos. El receptor traduce el regreso del ASCII estándar al juego de caracteres usados en la computadora del receptor.	JPEG, ASCII, EBCDIC, TIFF, GIF, PICT, Encriptamiento, MPEG, MIDI
Sesión (capa 5)	La capa de sesión define cómo empezar, controlar, y terminar conversaciones (llamadas sesiones). Esto incluye el mando y dirección de mensajes bidireccionales múltiples para que la aplicación pueda notificarse si sólo se completan alguna serie de mensajes. Esto permite a la capa de presentación tener una vista de un caudal entrante de datos. La capa de presentación puede presentarse con los datos si todos los flujos ocurren en algunos casos. Por ejemplo, una transacción de un cajero automático en la cual una persona retira dinero en efectivo de su cuenta corriente no debería cargarlos a su cuenta inmediatamente, ya que entonces fallaría antes de darle el dinero en efectivo, grabando la transacción aunque esa persona no haya recibido el dinero. La capa de sesión crea maneras de implicar qué flujos son parte de la misma sesión y qué flujos debe completar antes de que cualquiera sea considerado completo.	RPC, SQL, NFS, Nombres NetBios, AppleTalk ASP, DECnet SCP

Transporte (capa 4)	La capa 4 incluye la opción de protocolos que proporcionan o no la recuperación del error. Multiplexaje de los datos entrantes para flujos diferentes a las aplicaciones en el mismo host (por ejemplo, enchufes de TCP) también se realiza el reordenamiento del caudal de datos entrantes cuando los paquetes llegan en desorden.	TCP, UDP, SPX
Red (capa 3)	Esta capa define la entrega de paquetes de extremo-a-extremo. Para lograr esto, la capa de red define el direccionamiento lógico para que cualquier terminal pueda ser identificada. También define cómo funciona el ruteo y cómo se establecen las rutas para que los paquetes puedan ser entregados. La capa de red también define cómo fragmentar un paquete en paquetes más pequeños para acomodar los medios con el tamaño de unidad de transmisión máximos más pequeños. (Nota: No todos los protocolos de la Capa 3 usan la fragmentación.) La capa de red del modelo OSI define la mayoría de los detalles que un ruteador de Cisco considera al establecer las rutas. Por ejemplo, IP corre en un ruteador de Cisco y es responsable de examinar la dirección IP de un paquete, comparando esa dirección con la tabla de ruteo IP, fragmentando el paquete si la interfase saliente requiere los paquetes más pequeños, y haciendo cola el paquete a ser mandado a la interfase.	IP, IPX, AppleTalk DDP
Enlace de datos (capa 2)	Las especificaciones de la capa de enlace de datos (Capa 2) se preocupan por conseguir los datos a través de un enlace particular o medio. Los protocolos de enlace de datos definen la entrega a través de un enlace individual. Estos protocolos están necesariamente interesados con el tipo de medio de comunicación en cuestión; por ejemplo, 802.3 y 802.2 son las especificaciones técnicas de la IEEE, que es referido por OSI como protocolo de enlace de datos válidos (Capa 2). Estas especificaciones técnicas definen cómo trabaja Ethernet. Otros protocolos, como el Control de Enlace de Datos de Alto Nivel (High Level Data Link Control - HDLC) para un enlace WAN punto a punto, trata de los diferentes detalles de un enlace WAN. Como con otras especificaciones protocolares, OSI no crea a menudo ninguna especificación original para la capa de enlace de datos, pero en cambio confía en otras instituciones las cuales definen las normas como IEEE para crear los nuevos estándares para la capa de enlace de datos y la capa física.	IEEE 802.3/802.2, HDLC, Frame Relay, PPP, FDDI, ATM, IEEE 802.5/ 802.2
Física (capa 1)	Estas especificaciones técnicas de la capa física (Capa 1) que también son típicamente las normas de otras organizaciones, tratan de las características físicas del medio de transmisión. Los conectores, pines, y el uso de los pines, las corrientes eléctricas, codificación, y la modulación de luz, todas son parte de las diferentes especificaciones de la capa física. A veces se usan múltiples características técnicas para completar todos los detalles de la capa física. Por ejemplo, RJ-45 define la forma del conector y el número de alambres o pines en el cable. Ethernet y 802.3 definen el uso de los alambres 1, 2, 3, y 6. Así que, para usar cable nivel 5 con un conector RJ-45 para una conexión de Ethernet, se usan Ethernet y las especificaciones de la capa física del conector RJ-45.	EIA/TIA-232, V.35, EIA/TIA- 449, V.24, RJ45, Ethernet, 802.3, 802.5, FDDI, NRZI, NRZ, B8ZS

Algunos protocolos definen detalles de capas múltiples. Por ejemplo, la capa de aplicación TCP/IP pone en correlación a OSI en las capas 5 hasta la capa 7, el Sistema de Archivo de Red (NFS - Network File System) lleva a cabo elementos que coinciden con las tres capas.

Igualmente, las normas 802.3, 802.5, de Ethernet definen los detalles para el enlace de datos y las capas físicas. Las capas superiores no son tan importantes para los ingenieros especialistas en redes. Además, muchas personas de redes saben lo que es el modelo OSI, pero no necesitan memorizar todo sobre el tema. En la tabla 7 se muestra con suficiente detalle y explicación para una idea mas profunda de los componentes del modelo OSI. La Tabla 5, ofrece la descripción más condensada de las características de la capa y ejemplos.

Tabla 5

Nombre de la Capa OSI	Descripción Funcional	Ejemplos
Aplicación (Capa 7)	Interfase de Usuario	Telnet, HTTP
Presentación (Capa 6)	Cómo los datos son presentados Proceso especial, como la encriptación	JPEG, ASCII, EBCDIC
Sesión (Capa 5)	Los mantiene los datos separados de las diferentes aplicaciones	Los sistemas operativos y planificación de acceso de aplicación
Transporte (Capa 4)	Entrega Multiplexada fiable o no fiable	TCP, UDP, SPX
Red (Capa 3)	Direccionamiento lógico, el cual los ruteadores usan para la Determinación del camino	IP, IPX
Enlace de Datos (Capa 2)	La combinación de bits en bytes, y bytes en Tramas Acceso al medio usando direcciones MAC detección de error y recuperación del error	802.3/802.2, HDLC
Física (Capa 1)	Movimiento de los bits entre los dispositivos Especificación de voltaje, velocidad del alambre, y pines de salida del cable	EIA/TIA-232, V.35

1.3.3. Los Beneficios del modelo en capas y Conceptos

Pueden ganarse muchos beneficios del proceso de separar las funciones o tareas de conectar una red de computadoras en pedazos más pequeños, llamados capas, y definiendo las interfaces estandarizadas entre estas capas. Un beneficio obvio es que los protocolos individuales o capas son menos complejas y por consiguiente pueden definirse con gran detalle. La siguiente lista resume los beneficios de las especificaciones de los protocolos en capas

- Los humanos pueden discutir y pueden aprender más fácil acerca de muchos detalles de una especificación protocolar.
- Las interfaces estandarizadas entre las capas, facilitan la ingeniería modular. Los diferentes productos pueden proporcionar funciones de sólo algunas capas (como un ruteador en las Capas 1 a la 3), o algunos productos podrían proporcionar partes de las funciones del protocolo (como desarrolló Microsoft TCP/IP en Win95, o las aplicaciones de e-mail de Eudora, proporcionando apoyo TCP/IP en la capa de aplicación).
- Se crea un ambiente bueno para la interoperabilidad.
- La complejidad reducida permite cambios del programa más fáciles y la evolución del producto más rápida.
- Cada capa puede definir cabeceras y remolques alrededor de los datos del usuario. Cualquiera que examine las cabeceras y remolques para solucionar problemas, puede encontrar la cabecera o remolque para la Capa X y saber que tipo de información debe encontrarse.

Una capa usa los servicios de la capa inmediatamente debajo de ella. Por consiguiente, se hace más fácil recordar lo que cada capa hace. (Por ejemplo, la capa de red necesita entregar los

datos de extremo a extremo. Para hacer esto, usa la capa de enlace de datos para mandarlos hacia el próximo dispositivo sucesivo a lo largo de ese camino extremo-a-extremo.)

1.3.4. La interacción Entre las Capas de OSI

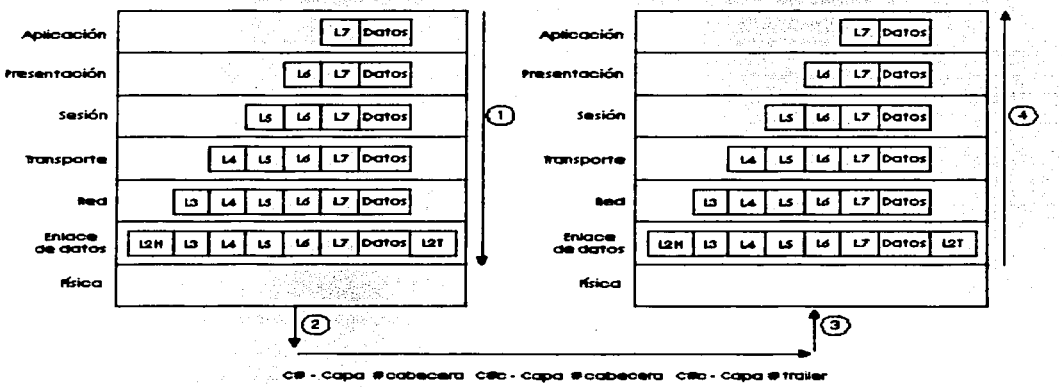
Los especialistas en redes trabajan frecuentemente con los conceptos de interacción y encapsulamiento, particularmente porque los ruteadores construyen las nuevas cabeceras y trailers del enlace de datos, para encapsular los paquetes hacia su destino.
El proceso de cómo las capas interactúan recíprocamente en la misma computadora, así como también, cómo la misma capa procesa en diferentes computadoras la comunicación con cada una de ellas, todas están interrelacionadas. Los productos de software o de hardware que llevan a cabo la lógica de alguna de las capas protocolares de OSI, proporcionan dos funciones generales:

- Cada capa proporciona un servicio a la capa sobre ella en la especificación protocolar.
- Cada capa comunica un poco de información con el mismo software de la capa o hardware en otras computadoras. En algunos casos, la otra computadora se conecta al mismos medio de comunicación; en otros casos, la otra computadora está en el otro extremo de la red.

1.3.5. Interacciones Entre las Capas Adyacentes en la Misma Computadora

Para proporcionar los servicios a la siguiente capa más alta, una capa debe saber sobre las interfaces estándares definidas entre las capas. Estas interfaces incluyen definiciones de qué Capa N +1 deben proporcionar a la Capa N para conseguir los servicios, así como qué Capa de información N debe proporcionar de regreso a la Capa N +1.
En la figura 6 se muestra una representación gráfica de dos computadoras y mantiene un telón de fondo excelente para una discusión de interacciones entre las capas en la misma computadora.

Figura 6 Ejemplo de la discusión de las interacciones de las capas adyacentes



Los datos son creados por alguna aplicación en el host A. Por ejemplo, se teclea un mensaje de e-mail por el usuario. Cada capa crea una cabecera y pasa los datos abajo a la siguiente capa. (Las flechas en Figura 6, Paso 1, denota el paso de datos entre las capas.) Pasando los datos abajo a la

siguiente capa implica que la capa mas baja necesita realizar algunos servicios para la capa más alta; para realizar estos servicios, la capa más baja agrega un poco de información la cabecera o trailer. Por ejemplo, la capa de transporte no toca los datos ni la cabecera; la capa de red agrega una cabecera con destino a la dirección correcta de la capa de red para que el paquete pueda entregarse a la otra computadora. Desde la perspectiva de cada capa, los bits después de esa cabecera de esa capa, son considerados como datos. Por ejemplo, la capa 4 considera la capa 5, 6, y 7 como cabeceras, junto con los datos del usuario originales, para ser un campo de datos grande. Después de que la aplicación crea los datos, el software y hardware llevan a cabo que cada capa realice su trabajo, mientras se agrega la cabecera apropiada y trailer. La capa física puede usar el medio para enviar una señal para la transmisión física, como se muestra en el paso 2 en Figura 6.

En el recibo (Paso 3), El host B empieza las interacciones de la capa adyacente en el host B. El lado correcto de la Figura 6 muestra una flecha que apunta al lado de la computadora (Paso 4), esto significa que los datos recibidos están procesándose conforme sube las capas. De hecho, pensando sobre lo que cada capa hace en el modelo OSI puede ayudarle a decidir qué información pudiera estar en cada cabecera. La secuencia siguiente perfila los elementos esenciales de procesar a cada capa y muestra cómo cada capa mas baja proporciona un servicio a la próxima capa más alta. Considere el recibo de datos por el host en el lado correcto de Figura 6:

Paso 1	La capa física (Capa 1) asegura la sincronización de los bits y acomoda el patrón binario recibido en el búfer. Notifica que los datos de la capa de enlace que una trama ha sido recibida después de descifrar la señal entrante en caudal de bits. Por consiguiente, la capa 1 ha proporcionado entrega de un caudal de bits por el medio.
Paso 2	La capa de enlace de datos examina la sucesión de cheque de trama (Frame Check Sequence - FCS) en el trailer para determinar si los errores ocurrieron en la transmisión (detección de error). Si un error ha ocurrido, la trama se desecha. (Algunos protocolos de enlace de datos realizan la recuperación de error, algunos no hacen.) Las direcciones del enlace de datos se examinan para que el host B pueda decidir si debe procesar los datos más allá. Si los datos se diseccionan hacia el host B, los datos entre la Capa 2 cabecera y trailer se da al software de la capa 3. El enlace de datos ha entregado los datos a través de ese enlace.
Paso 3	La capa de red (Capa 3) examina la dirección de destino. Si la dirección es la del host B, el proceso continúa (direccionamiento lógico) y los datos después de la cabecera de la capa 3, son dados al software de la capa de transporte (capa 4). La capa 3 ha proporcionado el servicio de entrega de extremo a extremo.
Paso 4	Si la recuperación de error fue una opción escogida para la capa de transporte (capa 4), los contadores identifican este pedazo de datos y son codificados en la cabecera de la capa 4 junto con la información del reconocimiento (recuperación de error). Después de la recuperación de error y pidiendo de nuevo los datos entrantes, el datos se dan a la capa de sesión.
Paso 5	La capa de sesión (capa 5) puede usarse para asegurar que una serie de mensajes se completan. Por ejemplo, estos datos no podrían tener sentido si los próximos cuatro intercambios no se completan. La cabecera de la capa 5 podría incluir campos que significan que éste es un medio flujo en una cadena, no un flujo final. Después de que la capa de sesión asegura que todos los flujos se completaron, pasa los datos después de la cabecera de la capa 5 al software de la capa 6.
Paso 6	La capa de presentación (capa 6) define y manipula el formato de los datos. Por ejemplo, si los datos son binarios en lugar de los datos de carácter, la cabecera denota ese hecho. El receptor no intenta convertir los datos usando los caracteres ASCII predeterminados puestos en el host B. Típicamente, este tipo de cabecera sólo es incluido para el flujo de inicialización, no con cada mensaje siendo transmitido (estructura de datos). Después de que el formato de los datos se han convertido, los datos (después de la cabecera de la capa 6) son pasados entonces al software de la capa de aplicación (Capa 7).
Paso 7	La capa de aplicación (capa 7) procesa la última cabecera y entonces puede examinar los datos verdaderos del usuario en el otro extremo. Esta cabecera significa el acuerdo para operar los parámetros por las aplicaciones en el host A y en el host B. Los títulos se usan para señalar los valores por todos los parámetros; por consiguiente,

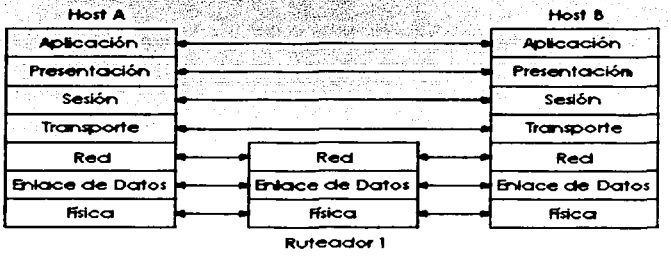
la cabecera típicamente se envía y sólo se recibe en momento de la inicialización de la aplicación. Por ejemplo, para la transferencia de archivos, el tamaño del archivo a ser transferido y los formatos usados se comunicarían (parámetros de aplicación)

1.3.6. Interacciones Entre las Mismas Capas en diferentes Computadoras

La capa N debe interactuar recíprocamente con la capa N en otra computadora para llevar a cabo sus funciones con éxito. Por ejemplo, la capa de transporte (capa 4) puede enviar los datos, pero si la otra computadora no reconoce que datos fueron recibidos, el remitente no sabrá cuándo realizar la recuperación error. Igualmente, la computadora transmisora codifica una dirección de destino en la cabecera de la capa de red (capa 3). Si los ruteadores intermedios no cooperan realizando su tarea en la capa de red, el paquete no se entregará al verdadero destino.
Para actuar recíprocamente con la misma capa en otra computadora, cada capa define una cabecera y, en algunos casos, un remolque. Las cabeceras y remolques son los bits adicionales de datos, creados por el software o el hardware de la computadora emisora los cuales son puestos antes o después de los datos dados a la capa N por la capa N+1.

La información necesitada por esta capa para comunicar con el mismo proceso de la capa en la otra computadora es codificada en la cabecera y el remolque. El software o hardware de la capa N de la computadora receptora interpreta la cabecera y remolque creados por la capa N de la computadora emisora, aprendiendo como esta siendo manejado el proceso de la capa N en este caso.
La figura 7 proporciona una perspectiva conceptual en las interacciones de la misma capa. La capa de aplicación en el host A se comunica con la capa de aplicación en el host B. Así como, las capas de transporte, sesión, y presentación en el host A y host B también se comunican. Las tres capas del fondo del modelo OSI tienen que ver con la entrega de los datos; el ruteador 1 está envuelto en ese proceso. Las capas de red, física y enlace de datos del host A, se comunican con las capas, física, enlace de datos y red del host B. Figura 7 proporciona una representación visual de los conceptos de interacción de la misma capa.

Figura 7 Interacción en las mismas capas en diferentes computadoras



1.3.7. Encapsulamiento de datos

El concepto de poner los datos detrás de las cabeceras para cada capa, se llama típicamente Encapsulamiento por la documentación de Cisco. Como se vio previamente en la Figura 7, cuando cada capa crea su cabecera, pone los datos dados en ella por la siguiente capa mas alta detrás de su propia cabecera, encapsulando los datos de la capa más alta. En el caso de un protocolo de enlace de datos (Capa 2), la cabecera y los datos de la capa 3 son puestos entre la cabecera de

la capa 2 y el remolque de la capa 2. La capa física no usa el encapsulamiento porque no usa cabeceras o remolques.
De nuevo, refiriéndose a la figura 7, el paso 1, de la lista siguiente describe el proceso de encapsulamiento de la creación de los datos del usuario, hasta que la señal física se codifica al Paso 2:

Paso 1 La aplicación ya ha creado los datos. La capa de la aplicación crea la cabecera de la aplicación y pone los datos detrás de ella. Esta estructura de datos, se pasa a la capa de presentación.

Paso 2 La capa de la presentación crea la cabecera de presentación y pone los datos detrás de ella. Esta estructura de los datos se pasa a la capa de la sesión.

Paso 3 La capa de la sesión crea la cabecera de sesión y pone los datos detrás de ella. Esta estructura de los datos se pasa a la capa de transporte.

Paso 4 La capa de transporte crea la cabecera de transporte y pone los datos detrás de ella. Esta estructura de los datos se pasa a la capa de la red.

Paso 5 La capa de la red crea la cabecera de la red y pone los datos detrás de él. Esta estructura de datos se pasa a la capa de enlace de datos.

Paso 6 La capa de enlace de datos crea la cabecera del enlace de datos y pone los datos detrás de ella. El trailer de enlace de datos se agrega al extremo de la estructura. Esta estructura de datos se pasa a la capa física.

Paso 7 La capa física codifica una señal en el medio para transmitir la trama.

El proceso de los siete pasos anteriores es exacto y de mucho significado para el modelo de las siete capas de OSI. Sin embargo, el encapsulamiento por cada capa no ocurre (típicamente) para cada transmisión de datos por la aplicación. Normalmente, las capas 5 a la 7 usan cabeceras durante la inicialización (y en ocasiones después de la inicialización), pero en la mayoría de los flujos, no hay ninguna cabecera en las capas 5, 6, o 7. Esto es porque no hay nueva información para intercambiar para cada flujo de datos.

El término LXPDU (Protocol Data Unit) dónde X representa el número de una de las capas, se usa para representar los bits que incluyen las cabeceras y remolques para esa capa, así como los datos encapsulados. Por ejemplo, un paquete IP es un L3PDU que incluye la cabecera IP y cualquier encapsulamiento de datos.

Paso 1 Creación de los datos – Esto simplemente significa que la aplicación tiene datos para enviar.

Paso 2 Empaquetamiento de los datos para el transporte - En otras palabras, la capa de transporte crea la cabecera de transporte y pone los datos detrás de el. El L4PDU se crea aquí.

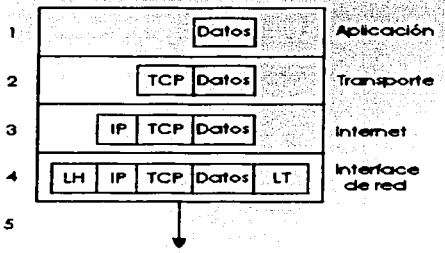
Paso 3 Agrega la dirección de destino a la capa de red - la capa de la red crea la cabecera de red que incluye la dirección de la capa de red, y pone los datos (L4PDU) detrás de el. En otros términos, el L3PDU se crea aquí.

Paso 4 Agrega la dirección de destino a la capa de enlace de datos - La capa de enlace de datos cera la cabecera de enlace de datos, pone los datos (L3PDU) detrás de el, y pone el remolque de enlace de datos al final. En otras palabras, el L2PDU se crea aquí.

Paso 5 Transmite los bits - La capa física codifica una señal en el medio para transmitir la trama

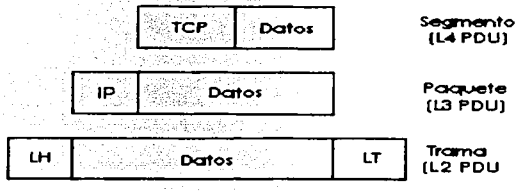
Este proceso de cinco pasos sucede para acoplar muy bien al modelo de red de TCP/IP. La figura 8 ilustra el concepto; los números mostrados representan cada uno de los cinco pasos.

Figura 8 Los cinco pasos de la encapsulamiento de datos



Alguna terminología común es necesitada para discutir los datos que esta procesando una capa en particular. La capa N (Protocol Data Unit - PDU - unidad de datos del protocolo), es un término usado para describir un juego de bytes que incluyen la cabecera y remolque de la capa N, todas las cabeceras encapsuladas, y los datos de usuario. Desde la perspectiva de la capa N, las cabeceras y los datos de usuario de la capa superior, forman un gran campo de datos o de información. Algunos otros términos también describen algunas de estas PDUs. La Capa 2 PDU (incluyendo la cabecera y el remolque del enlace de datos) se llama trama. Semejantemente, la Capa 3 PDU se llama paquete, o a veces datagrama. Finalmente, la Capa 4 PDU se llama segmento. La figura 9 ilustra la construcción de tramas, paquetes, y segmentos y las diferentes perspectivas de las capas en lo que se considera que son datos.

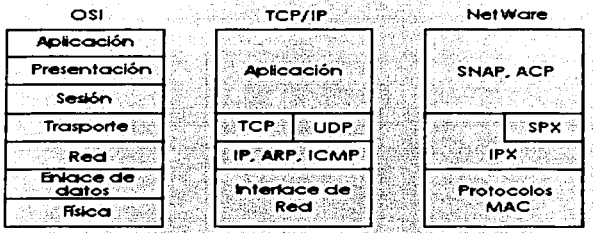
Figura 9 Tramas paquetes y segmentos



1.3.8. Los protocolos TCP/IP y NetWare

En esta sección se compara TCP/IP, Novell, y OSI. La meta es proporcionar una visión en lo que realmente significan algunos términos usados popularmente. En particular, ruteo, se define como un proceso de la capa 3; esta sección repasa cómo ese término se relaciona con TCP/IP y NetWare. Para una mejor perspectiva, la figura 10, muestra las capas de estos dos protocolos comparados con OSI.

Figura 10 Protocolos OSI, TCP/IP y NetWare



Como se ilustra en la figura 10, los protocolos IP e IPX tienen una semejanza mas cercana con la capa de red de OSI (capa 3). Claramente, IP está en la capa 2 de TCP/IP, pero para el uso consistente de terminología, se llama normalmente protocolo de Capa 3 porque sus funciones se asemejan estrechamente con la capa 3 de OSI. IP e IPX definen el direccionamiento lógico, ruteo, el aprendizaje la información de, ruteo y las reglas de la entrega de extremo-a-extremo.

Como con las Capas 1 y 2 de OSI (física y enlace de datos, respectivamente), las más bajas capas de cada pila simplemente se refieren a otras especificaciones muy conocidas. Por ejemplo, todas las capas más bajas soportan las normas de IEEE para Ethernet y Token Ring, la norma ANSI para FDDI, la norma de ITU para ISDN, y los protocolos Frame Relay especificados por el Foro Frame Relay (Frame Relay Forum), ANSI, y la ITU. Las pilas de los protocolos pueden acomodarse en otra desarrollando las especificaciones de la capa 1 y 2 más fácilmente, refiriéndose al salir las normas internacionales en lugar de intentar desarrollar estas normas.

1.3.9. Funciones de la capa de Transporte de OSI

La capa de transporte (Capa 4) define varias funciones. Dos características importantes cubiertas en este capítulo, son recuperación de error y control de flujo. Los ruteadores desechan los paquetes por muchas razones, incluso los errores de bit, congestión que ha causado una falta de espacio en el búfer, y en casos en donde ninguna ruta correcta es conocida. La capa de transporte puede proveer la retransmisión (recuperación de error) y puede ayudar a evitar la congestión (control de flujo). Los protocolos de la capa de transporte se categorizan típicamente como orientado a conexión o no orientado a conexión.

1.4. Funciones de la capa de enlace de Datos de OSI

Es necesario entender ambos conceptos abstractos acerca de las capas de OSI y casos en particular de tales protocolos. Esta sección examina cuatro protocolos diferentes: Ethernet, Token Ring, HDLC, y Frame Relay. Una definición generalizada de la función de un protocolo de enlace de datos se usará para guiarlo a través de la comparación de estos cuatro protocolos. Esta definición podría usarse para examinar cualquier otro protocolo de enlace de datos. Los cuatro componentes de esta definición de las funciones de los protocolos de enlace de datos (Capa 2) son como sigue

- Arbitraje - Determina cuando es apropiado usar el medio físico.
- Direccionamiento - Se asegura que el recipiente(s) correcto recibe y procesa los datos que se le envían.
- Detección de error - Determina si los datos hicieron el viaje con éxito a través del medio.
- Identificando los Datos encapsulados - Determina el tipo de cabecera que sigue a la cabecera de enlace de datos. Esta característica es incluida en un subconjunto de protocolos de enlace de datos.

Ethernet y Token Ring son dos protocolos populares LAN de capa 2. Estos protocolos se definen por la IEEE en las especificaciones 802.3 y 802.5, respectivamente. Porque 802.3 y 802.5 definen cómo una estación accesa al medio de comunicación, la IEEE llama estos protocolos, protocolos de Control de Acceso al Medio (Media Access Control - MAC). También, ambas especificaciones, 802.3 y 802.5 llaman el uso de otra especificación de IEEE como una parte separada de la capa de enlace de datos llamada 802.2 Control de Enlace Lógico (Logical Link Control - LLC). 802.2 es determinadamente diseñado para proporcionar las funciones comunes para Ethernet y Token Ring considerando que 802.3 y 802.5 se diseñaron específicamente para funciones de enlace de datos pertinentes a Ethernet o Token Ring.
Las normas de Ethernet antes de que la IEEE creara la norma 802.3, se llamo DIX Ethernet por un tiempo (las letras DIX representan Digital, Intel, y Xerox). DIX Versión 2 define las funciones similares para ambas especificaciones 802.3 y 802.2.

HDLC es el protocolo de enlace de datos predeterminado (encapsulamiento) en las interfaces seriales de los ruteadores Cisco. Las cabeceras Frame Relay son coincidentemente basadas en la especificación de HDLC, pero Frame Relay fue creado para las redes multiacceso (con más de dos dispositivos). Las diferencias claras entre Frame Relay y HDLC proporcionan un buen telón para examinar las funciones del enlace de datos de la capa (Capa 2).

1ª Función del enlace de datos: El arbitraje

El arbitraje sólo se necesita cuando hay instantes de tiempo en los que no es apropiado enviar los datos por el medio de comunicación. Las LAN fueron definidas originalmente como medios compartidos en los que cada dispositivo debe esperar el tiempo apropiado para enviar los datos. Las especificaciones técnicas para estos protocolos de enlace de datos, definen cómo arbitrar el uso del medio físico.
Ethernet usa el algoritmo de Acceso Múltiple Sensible a la Portadora con detección de colisiones (Carrier Sense Multiple Access Collision Detect - CSMA/CD) para el arbitraje. El algoritmo básico usado por Ethernet cuando hay datos para ser enviados consiste en los siguientes pasos

Paso 1 Escuchar para averiguar si una trama está recibiéndose actualmente.
Paso 2 Si ninguna otra trama está en el Ethernet, enviar.
Paso 3 Si otra trama está en el Ethernet, esperar y entonces escuchar de nuevo.
Paso 4 Mientras se esta enviando, si una colisión ocurre, detener, esperar, y escuchar de nuevo.

Con Token Ring, es usado un mecanismo totalmente diferente. Una trama Token libre rueda alrededor del anillo mientras ningún dispositivo tiene datos para enviar. Al enviar, un dispositivo exige que el Token Libre lo que realmente significa cambiar los bits en la cabecera del 802.5 para que

significique "token ocupado". Los datos se ponen entonces en el anillo después de la cabecera Token Ring. El algoritmo básico para usar un Token Ring cuando hay datos para ser enviados consiste en los pasos siguientes:

Paso 1 Escuchar el paso del Token.
Paso 2 Si el Token está ocupado, escuchar para el próximo Token.
Paso 3 Si el Token esta libre, marque el Token como un Token ocupado, y envíe los datos hacia el anillo.
Paso 4 Cuando la cabecera con el regreso del Token ocupado hacia el transmisor de esa trama, después de completar una revolución completa alrededor del anillo, el remitente quita los datos del anillo.
Paso 5 El dispositivo envía un Token libre para permitir a otra estación enviar una trama.

Con el arbitraje HDLC no es un problema hoy. HDLC se usa en enlaces de punto a punto que son típicamente circuitos full-duplex (cuatro alambres). En otros términos, cualquier punto final puede enviar cuando quiera. De una perspectiva física, Frame Relay se comprende de una línea arrendada entre un ruteador y el switch Frame Relay. Estos enlaces también son enlaces típicamente full-duplex, por los que no se necesita ningún arbitraje. La red Frame Relay es compartida entre muchos dispositivos DTE (Equipos Terminales de Datos), considerando que el enlace de acceso no es compartido, entonces el arbitraje del medio no es un problema.

La palabra "trama" se refiere a las partes particulares de los datos como enviados en un enlace. En particular, la trama implica que la cabecera de enlace de datos y el remolque son parte de los bits siendo examinados y discutidos. La figura 15 muestra las tramas para los cuatro protocolos de enlace de datos

Figura 15 Formatos populares de tramas

802.3	802.2	Datos	802.3
802.5	802.2	Datos	802.5

HDLC	Datos	HDLC
F. R.	Datos	F. R.

2ª Función de enlace de datos: Direccionamiento

Se requiere que se dominen los formatos y significados del enlace de datos y direcciones de la capa de red. El direccionamiento se necesita en las LANs porque puede haber muchos posibles destinatarios, esto es, podría haber más de dos dispositivos en el enlace. Porque las LANs son un medio de transmisión, esto significa que todos los dispositivos en el medio reciben los mismos datos, cada destinatario debe hacer la pregunta, "¿Esta trama es para mi?".
Con Ethernet y Token Ring, las direcciones son muy similares. Cada una usa el Control de Acceso al Medio (MAC) direcciones que son de 6 bytes de largo y que se representan como un número de hexadecimal de 12 dígitos. La tabla 12 resume la mayoría de los detalles sobre las direcciones MAC.

Tabla 12

Direccionamiento LAN, Términos y Características	**Descripción**
MAC	Control de Acceso al Medio. 802.3 (Ethernet) y 802.5 (Token Ring) es las subcapas de MAC de estos dos protocolos LAN de enlace de datos.
Direcciones Ethernet, NIC, LAN, Token Ring , y de la tarjeta,	Otros nombres usados a menudo en lugar de direcciones MAC. Estos términos describen la dirección de 6 bytes de la tarjeta de la interfase LAN.

Dirección quemada	La dirección de 6 bytes asignada por el distribuidor que hace la tarjeta. Normalmente se quema en una ROM o EEPROM en la tarjeta LAN y empieza con un identificador único organizacional (OUI) de 3 bytes asignado por la IEEE
Dirección localmente administrada	Vía configuración, una dirección que se usa en lugar del quemar la dirección en la tarjeta.
Dirección unicast	Término elegante para una dirección MAC que representa una sola interfase de LAN. Cast
Dirección broadcast	Una dirección que significa "todos los dispositivos que residen en esta LAN ahora".
Dirección multicast	No válido en Token Ring. En Ethernet, una dirección de multicast implica algún subconjunto de todos los dispositivos actualmente en la LAN.
Dirección funcional	No válido en Ethernet. En Token Ring, estas direcciones se reservan para representar los dispositivo(s) en el anillo realizando una función en particular. Por ejemplo, todos los puentes de ruta fuente, suministran el número del anillo a otros dispositivos; para hacer que, cada uno de ellos escuchen la dirección funcional del Servidor de Parámetro del Anillo (RPS)

HDLC incluye un campo de dirección sin sentido porque sólo se usa solo en los enlaces seriales de punto a punto. El destinatario es implícito; si un dispositivo enviara una trama, el otro dispositivo es el único destinatario intencional posible.

Con Frame Relay, hay un enlace físico que tiene muchos circuitos lógicos llamados circuitos virtuales (Virtual Channel - VC). El campo de dirección en Frame Relay, define un Identificador de Conexión de Enlace de Datos (Data Link Connection Identifier - DLCI), el cual identifica cada VC. Por ejemplo, en la figura 16, el switch de Frame Relay el cual se conecta al el ruteador Timbuktu, recibe las tramas, el switch remite la trama a Kalamazoo o Este de Egipto basándose en el DLCI que identifica a cada VC. Así que, Timbuktu tiene una conexión física pero múltiples conexiones lógicas.

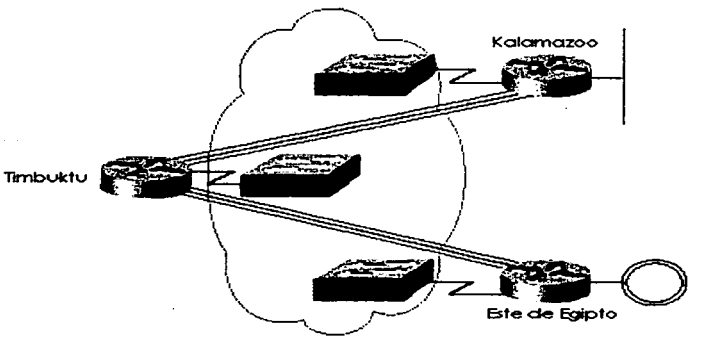


Figura 16 Red Frame Relay

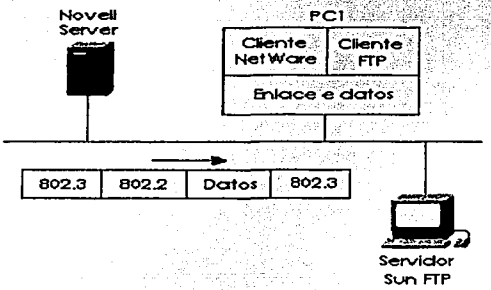
3ª Función de enlace de datos: Detección de error

La detección de error simplemente es el proceso de aprender si los errores de los bits ocurrieron durante la transmisión de la trama. Para hacer esto, la mayoría de enlaces de datos incluyen un campo de secuencia de chequeo de trama (FCS) o un chequeo de redundancia cíclica (Cyclical redundancy Check - CRC) en el remolque de enlace de datos. Este campo contiene un valor que es el resultado de una fórmula matemática aplicada a los datos en la trama. El valor de FCS calculado y enviado por el remitente debe coincidir con el valor calculado por el receptor. Todos los cuatro enlaces de los datos discutidos en esta sección contienen un campo de FCS en el remolque de la trama.

4ª Función Enlace de Datos: Identificando los Datos Encapsulados

Finalmente, la cuarta parte de un enlace de datos, identifica el contenido de los datos presentados en la trama. La figura 17 muestra la utilidad de esta característica.

Figura 17 Multiplexaje usando tipo enlace de datos y campos de protocolo

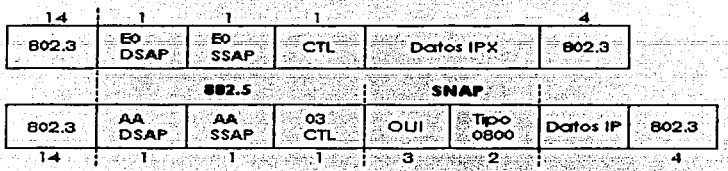


Cuándo la PC1 recibe los datos, ¿le da los datos al software de TCP/IP o al cliente NetWare? Claro, eso depende de lo que está dentro del campo de los datos. Si los datos vinieran del servidor Novell, entonces la PC1 le da los datos fuera del código del cliente NetWare. Si los datos vienen del servidor Sun FTP, la PC1 lo da fuera del código de TCP/IP.

Ethernet y Token Ring 802.2 LLC, proporcionan un campo en su cabecera para identificar el tipo de datos en el campo de datos. La PC1 recibe tramas que básicamente se parecen a las dos mostradas en la figura 18. Cada cabrera de enlace de datos tiene un campo con un código que significa IP, o IPX, o alguna otra designación que define el tipo de cabecera de protocolo que sigue. El primer artículo para examinar en la cabecera es el 802.2 campo DSAP. En la primera trama en la figura 18, el campo del Punto de Acceso de Servicio de Destino (Destination Service Access Point - DSAP) tiene un valor de E0, que significa que la próxima cabecera es una cabecera Novell IPX. En la segunda trama, el campo de DSAP es AA que implica que sigue una cabecera SNAP. Luego, el tipo de campo en la cabecera del Protocolo de Acceso de Subred (SubNetork Access Protocol - SNAP), la cual tiene un valor de 0800 y significa que la próxima cabecera es una cabecera IP.

Similarmente, HDLC y Frame Relay necesitan identificar los volúmenes del campo de datos. Claro, no es típico tener los dispositivos del extremo del usuario conectados a cualquiera de estos tipos de enlace de datos. En este caso, los ruteadores proporcionan un ejemplo mas típicamente encontrado en la mayoría de los ambientes WAN, como se muestra en la figura 19.

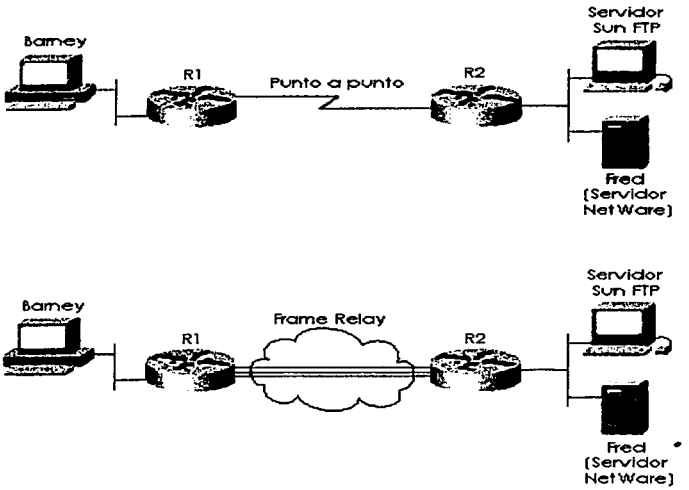
Figura 18 Tipos de campos 802.2 SAP y SNAP



Refiriéndose a la parte de arriba de la figura 19, si Barney está usando FTP para transferir los archivos al sistema Sun, y también se conecta al servidor NetWare (Fred) usando IPX, entonces Barney generará tráfico TCP/IP y NetWare. Como este tráfico pasa encima del enlace controlado HDLC, R2 necesitará saber si un paquete IP o IPX sigue la cabecera HDLC. Principalmente, esto es para que el ruteador pueda encontrar la dirección de destino, asumiendo que su longitud es de 32 o 80 bits, realizando el chequeo en la tabla de ruteo correcta (ID o IPX), tomando la decisión de la asignación de ruta correcta.

HDLC no proporciona un mecanismo para identificar el tipo de paquete en el campo de datos. El IOS agrega un campo de su propiedad de 2 bytes inmediatamente después de la cabecera HDLC que identifica los contenidos de los datos. Como se muestra en el fondo de figura 19, los switches Frame Relay intermedios no cuidan lo que esta dentro del campo de datos.

Figura 19 Identificando protocolos sobre HDLC y Frame Relay



El ruteador receptor, R2, quiere las mismas razones que R2 quiere cuando se esta usando HDLC, eso es lo que el ruteador receptor necesita saber si un paquete IP o IPX sigue la cabecera de Frame Relay. Las cabeceras Frame Relay no se dirigieron a este problema, originalmente porque los títulos eran basados en HDLC. Sin embargo, el IETF crea una especificación que llamó RFC 1490 eso definió las cabeceras adicionales que siguieron a la cabecera Frame Relay. Estas cabeceras incluyen varios campos que pueden usarse para identificar los datos para que el dispositivo receptor sepa que, tipo esta oculto dentro.
El ITU y ANSI recopilaron las especificaciones de RFC 1490 y lo agregaron a sus normas Frame Relay oficiales: El ITU T1.617 Anexo F y ANSI Q.933 Anexo E, respectivamente.

La Figura 20 muestra los campos que identifican el tipo de protocolo encontrados en el campo de datos.

Como se ve en Figura 20, un campo del tipo protocolo viene después del campo de control HDLC. En el ejemplo de Frame Relay, existen cuatro opciones diferentes para identificar el tipo de datos dentro de la trama. RFC 2427, que pone obsoleta la RFC 1490

La tabla 13 resume las opciones diferentes para codificar los tipos de protocolos para cada uno de los cuatro protocolos de enlace de datos. Note que la longitud de algunos de estos campos es de sólo 1 byte, el cual históricamente ha llevado a la incorporación de otras cabeceras. Por ejemplo, la cabecera SNAP contiene un campo del tipo de 2 bytes porque un campo DASP de 1 byte no es lo bastante grande para numerar todas las opciones disponibles para saber qué tipo de protocolo está dentro de los datos.

Figura 20 Tipo de campo de los protocolos HDLC y Frame Relay

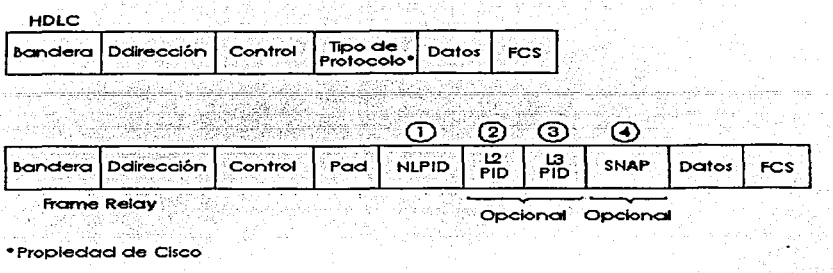


Tabla 13 Diferentes Opciones para codificar los Tipos de Protocolo para Cada uno de los Cuatro Ejemplos de Protocolos de enlace de datos.

Protocolo de Enlace de Datos	**Campo**	**Cabecera en la cual se encuentra**	Tamaño
802.3 Ethernet Y 802.5 Token Ring	DSAP	Cabecera 802.2	1 byte
802.3 Ethernet Y 802.5 Token Ring	DSAP	Cabecera 802.2	1 byte
802.3 Ethernet Y 802.5 Token Ring	Tipo de Protocolo	Cabecera SNAP	2 bytes
Ethernet (DIX)	Ethertype	Cabecera Ethernet	2 bytes
HDLC	Campo de identificación protocolar propietario de Cisco	Cabecera Extra Cisco	2 bytes
Frame Relay RFC 2427	NLPID	RFC 1490	1 byte
Frame Relay RFC 2427	Identificación de Protocolo de capa 1, 2 o 3	Q.933	2 bytes cada una
Frame Relay RFC 2427	Tipo de Protocolo SNAP	Cabecera SNAP	2 bytes

Resumen: Funciones del enlace de datos

La Tabla 14 resume las funciones básicas de los protocolos de enlace de datos:

Tabla 14 Funciones de los Protocolos de enlace de datos

Función	**Ethernet**	**Token Ring**	**HDLC**	**Frame Relay**
Arbitraje	Algoritmo CSMA/CD (parte de MAC)	Token passing (parte de MAC)	—	—
Direccionamiento	Fuente y destino de las direcciones MAC	Fuente y destino de las direcciones MAC	Dirección de solo 1 byte; insignificante en los enlaces punto a punto	DLCI usado para identificar circuitos virtuales
Identificando el contenido de los datos	802.2 DSAP, cabecera SNAP, o Ethertype, como sea necesario.	802.2 DSAP o cabecera SNAP, como sea necesario.	Campo del Tipo de propietario	Cabeceras RFC 1490/2427, con NLPID capa 2, e identificador de protocolo de capa 3 o cabecera SNAP

1.5. Funciones de la capa de red de OSI

Las dos funciones claves para cualquier Protocolo de Capa 3 ron el ruteo y el direccionamiento. Estas dos funciones se entrelazan y se entienden mejor considerando los dos al mismo tiempo.
El direccionamiento de la capa de red (Capa 3) se cubrirá con bastante profundidad ara describir las direcciones IP, IPX, y AppleTalk. También, ahora esos enlaces de datos y direcciones de la capa de red se unen, se han cubierto las direcciones de la capa de red en este capítulo, esta sección emprende una comparación de los dos también.

1.5.1. Ruteo

El ruteo puede pensarse como un proceso de tres pasos, como se muestra en la Figura 21. Pensando acerca del ruteo en estos tres pasos separados, ayudan a hacer algunos de estos detalles más obvios. Sin embargo, la mayoría de las personas no pensaran en el ruteo como un proceso de tres pasos cuando están haciendo su trabajo, esto es simplemente una herramienta para hacer algunos puntos más claramente

Figura 21 Los tres pasos del ruteo

Como se ilustra en figura 21, los tres pasos del ruteo incluyen lo siguiente:

Paso 1	Enviando los datos de la computadora fuente a algún ruteador cercano
Paso 2	Entregando los datos de un ruteador cerca de la fuente a un ruteador cerca del destino
Paso 3	Entregando los datos del ruteador cerca del destino a la computadora de destino final

Paso 1: Enviando Los Datos a un Ruteador Cercano

El creador de los datos, quien también es el remitente de los datos, decide enviar los datos a un dispositivo en otro grupo. Un mecanismo debe estar en el lugar para que el remitente conozca algún ruteador en un enlace de datos común con el remitente para asegurar que esos datos puedan ser enviados a ese ruteador. El remitente envía una trama de enlace de datos a través del medio hacia el ruteador cercano; esta trama incluye el paquete en la porción de datos de la trama. Esa trama usa el direccionamiento de enlace de datos (Capa 2) en la cabecera de enlace de datos para asegurar que el ruteador cercano recibe la trama.

Paso 2: Ruteo de Datos a través de la Red

La tabla de ruteo para ese tipo de protocolo de la capa de red en particular es nada más que una lista de agrupaciones de direcciones de la capa de red. Como se mostrará en la tabla 15 después en esta sección, estas agrupaciones varían basadas en el tipo de protocolo de la capa de red. El ruteador compara la dirección de destino de la capa de red en el paquete hacia las entradas de la memoria de la tabla de ruteo, y se hace una comparación. Esta comparación entrante en la tabla de ruteo le dice a este ruteador dónde remitir el siguiente paquete.

Cualquier ruteador intermedio repite el mismo proceso. La dirección en el paquete identifica el grupo en que el destino reside. Se busca en la tabla de ruteo para una entrada que coincida la cual le dice a este ruteador dónde remitir próximo al paquete. En el futuro, el paquete se entrega al ruteador conectado a la red o subnet del host de destino, como previamente se mostró en la Figura 21.

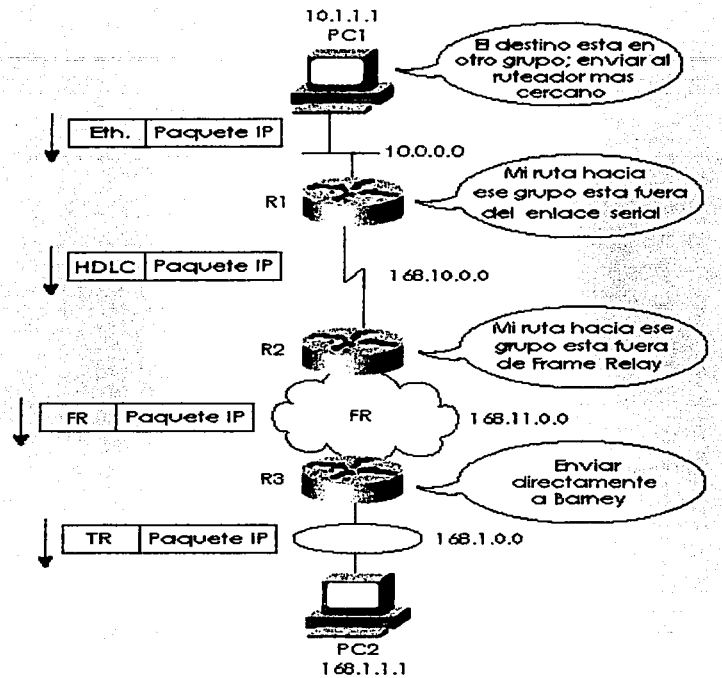
1.5.2. Un Comentario Sobre los Enlaces de Datos

Ya que los ruteadores construyen nuevas cabeceras y remolques de enlace de datos, y porque las nuevas cabeceras contienen direcciones de enlace de datos, los ruteadores deben tener alguna manera de decidir qué direcciones de enlace de datos usar. Un ejemplo de cómo el ruteador determina que direcciones de enlace de datos usar, es el Protocolo de Resolución de Dirección IP (Address Resolution Protocol - ARP).
ARP es usado para aprender dinámicamente las direcciones de enlace de datos de algún host IP.

Un ejemplo específico de TCP/IP será útil para solidificar los conceptos detrás del ruteo. Imagine que la PC1 está enviando los paquetes a la PC2. La figura 22 proporciona un ejemplo de una red para que se pueda repasar el proceso de ruteo.

La lógica detrás del proceso de ruteo de los tres pasos anteriores se describe en los pasos siguientes. Los pasos A y B que siguen describen el primero de los tres pasos del ruteo en este ejemplo. Los pasos C, D, E, F, y G corresponden al paso 2. Finalmente, el paso H que corresponde al paso 3 de ruteo.

Figura 22 Lógica de ruteo y encapsulamiento – PC 1 envía hacia la PC2



Paso A

La PC1 necesita conocer a su ruteador más cercano. La PC1 conoce las primeras direcciones IP de R1 teniendo o un ruteador predeterminado o una pasarela predefinida configurada. El ruteador predeterminado definido en algún host es el ruteador el cual ese host remite paquetes que se destinan para las otras subredes que las subredes directamente conectadas. Alternativamente, la PC1 puede aprender las direcciones IP del R1 usando El Protocolo de Configuración de Host Dinámico (Dynamic Host Configuration Protocol DHCP), se puede asumir que un ruteador predefinido con 10.1.1.100 se configura en la PC1 y que es la dirección Ethernet IP de R1.

Paso B

La PC1 necesita conocer la dirección MAC Ethernet de R1 antes de que la PC1 pueda terminar de construir la cabecera Ethernet (vea la figura 27). En el caso de TCP/IP, el proceso ARP se usa para aprender la dirección MAC de R1 dinámicamente. Cuando la dirección MAC de R1 es conocida, la PC1 completa la cabecera Ethernet con la dirección de destino MAC siendo la dirección MAC de R1.

Paso C	En el paso 2 del proceso de ruteo, el ruteador tiene muchos artículos para considerar. Primero, la trama entrante (interfase Ethernet) es procesada solo si el FCS de Ethernet es aprobado y la dirección MAC del ruteador está en el campo de dirección de destino. Entonces, el campo del tipo de protocolo apropiado se examina para que R1 sepa qué tipo de paquete está en la porción de los datos de la trama. A estas alturas, R1 desecha la cabecera Ethernet y el trailer.
Paso D	La siguiente parte del Paso 2 involucra el hallar una entrada en la tabla de ruteo para red 168.1.0.0, la red de la que la PC2 es un miembro. En este caso, la ruta en el R1 se refiere a 168.1.0.0 y lista la interfase serial de R1 como la interfase por la cual remitir el paquete.
Paso E	Para completar el paso 2, R2 construye una cabecera y trailer HDLC para poner alrededor del paquete IP. Ya que el enlace de datos HDLC usan el mismo campo de dirección cada vez, no se necesita ningún proceso como ARP para permitirle al R1 construir la cabecera HDLC.
Paso F	El paso 2 de ruteo se repite por el R2 cuando recibe la trama HDLC. El HDLC FCS se verifica; el tipo de campo se examina para aprender que el paquete dentro de la trama es un paquete IP, y entonces la cabecera HDLC y el trailer se desechan. La tabla de ruteo IP en R2 se examina para la red 168.1.0.0, y se hace una comparación. La entrada se dirige al R2 para remitir el paquete a su interfase serial Frame Relay. La entrada ruteo también identifica las siguientes direcciones IP, llamadas direcciones IP del R3 en el otro extremo del circuito virtual (VC) Frame Relay.
Paso G	Antes de que el R2 pueda completar su Paso 2 de este ruteo extremo a extremo el algoritmo, del R2 debe construir una cabecera y trailer Frame Relay. Antes de que pueda completar la tarea, el DLCI correcto para el VC hacia el R3 debe ser decidido. En la mayoría de los casos de hoy, el proceso dinámico inverso ARP habrá asociado la dirección IP del R3 con la que usa el DLCI del R2. Para enviar las tramas hacia el R3. Con esa información de mapeo, el R2 puede completar la cabecera Frame Relay puede enviar la trama al R3.
Paso H	El paso 3 del algoritmo original es realizado por el R3. Como el R1 y el R2 antes de él, R3 verifica el FCS en trailer de enlace de datos, mira el tipo de campo para decidir si el paquete dentro de la trama es un paquete IP, y entonces desechar la cabecera y el trailer Frame Relay. La entrada de la tabla de ruteo para 168.1.0.0 muestra que la interfase de salida es la interfase Token Ring del R3. Sin embargo, no hay ninguna dirección próxima IP del ruteador, porque no hay ninguna necesidad de remitir el paquete a otro ruteador. El R3 simplemente necesita construir una cabecera y trailer Token Ring y remitir la trama que contiene el paquete original a la PC2. Antes de que el R3 pueda terminar de construir la cabecera Token Ring, un IP ARP debe ser usado para encontrar la dirección MAC de la PC2 (asumiendo que ese R3 no tiene ya esa información en su memoria caché IP ARP).

1.5.3. Direccionamiento en la Capa de Red (Capa 3)

Las direcciones de la capa de red son agrupaciones basadas en la locación física en una red. Las reglas difieren para algunos protocolos de la capa de red, pero el concepto de la agrupación es idéntico para IP, IPX, y AppleTalk. En cada uno de éstos los protocolos de la capa de red, no pueden separarse todos los dispositivos con las direcciones en el mismo grupo, no pueden ser separadas de cada uno de los otros por un ruteador que se configure para dirigir ese protocolo, respectivamente. Declarado diferentemente, todos los dispositivos en el mismo grupo (subred/red/rango de cable) deben conectarse al mismo enlace de datos; por ejemplo, todos los dispositivos deben conectarse al mismo Ethernet. El ruteo confía en el hecho de que las direcciones de la capa 3 son agrupadas juntas. Las tablas de ruteo para cada protocolo de la capa de red pueden referirse al grupo, no a cada dirección individual. Imagine un Ethernet con 100 clientes de Novell. Un ruteador que necesita remitir los paquetes a cualquiera de esos clientes, necesita solo una entrada en su tabla de ruteo IPX. Si esos clientes no fueran requeridos para ser atados al mismo enlace de datos, y si no hubiera manera de codificar el número de red IPX en la dirección IPX del cliente, el ruteo no sería capaz de usar simplemente una entrada en la tabla.

Este hecho básico es una de las razones importantes por la que los ruteadores, usando el ruteo como se definió por la capa de red (Capa 3), puede incrementarse para permitir las decenas, cientos y miles de dispositivos.

Con eso en mente, la mayoría de los esquemas de direccionamiento de la capa de red (Capa 3), se crearon con las metas siguientes:

- El espacio de dirección debe ser bastante grande para acomodar la más grande red para la cual los diseñadores imaginaron que el protocolo se usaría.
- Las direcciones deben permitir la asignación única para que la oportunidad de duplicación de direcciones sea pequeña o no exista
- La estructura de las direcciones debe tener alguna agrupación implicada que se considere que muchas direcciones estén en el mismo grupo.
- En algunos casos se desea, la asignación de direcciones dinámicas.

Una gran analogía para este concepto de direccionamiento de red es el esquema usado por el Servicio Postal Estadounidense. En lugar de estar involucrado con los planes de cada pequeña comunidad para como nombrar las nuevas calles, la oficina de correos simplemente tiene una oficina cercana con un código postal. El resto de las oficinas de correos del país están preparadas para enviar el correo a los nuevos negocios y residencias en las nuevas calles; ellos solo se preocupan del código postal que ellos ya saben. Es el trabajo del jefe postal local que asigne a un portador entregar y recoger el correo con esas nuevas calles. Puede haber centenares de Calles principales en los diferentes códigos postales, pero solo hay un código postal, la dirección es única y con un porcentaje alto de éxito.

1.5.4. Ejemplo de capa 3 Estructuras de las Direcciones

Cada estructura de las direcciones de la Capa 3 contiene por lo menos dos partes. Una (o más) partes la principio de la dirección funciona como el código postal y esencialmente identifica la agrupación. Todos los casos de direcciones con el mismo valor en estos primeros bits de la dirección son consideradas para estar en el mismo grupo por ejemplo, la misma subred IP o red IPX o cable de rango AppleTalk. La última parte de los actos de dirección como direcciones locales, identificando ese dispositivo singularmente en ese grupo en particular. La tabla 15 perfila varias estructuras de dirección de la capa 3.

Tabla 15

Protocolo	Tamaño de las direcciones (En bits)	El nombre y Tamaño de Agrupaciones de Campo	Nombre y tamaño del campo de direcciones locales
IP	32	Red o subred (variable, entre 8 y 30 bits)	Host (variable, entre 2 y 24 bits)
IPX	80	Red (32)	Nodo (48)
AppleTalk	24	Red (16) (Consecutivamente valores numerados en este campo pueden ser combinados en un grupo, llamado rango del cable.)	Nodo (8)
OSI	Variable	Muchos formatos, muchos tamaños	Parte específica de dominio (DSP) (típicamente 56, incluyendo NSAP)

1.5.5. Protocolos de ruteo

Convenientemente, las tablas ruteo en el ejemplo basado en la Figura 22, todos ya tenían la información de ruteo correcta en sus tablas de ruteo. En la mayoría de los casos, estas entradas se construyen dinámicamente por el uso de un protocolo de ruteo. Los protocolos de ruteo definen la estructura y procedimientos del mensaje, como cualquier otro protocolo. Con los protocolos de ruteo, sin embargo, la meta es no ayudar con la entrega de datos del usuario final, la meta es llenar la tabla de ruteo con todos los grupos destino conocidos y con la mejor ruta para alcanzar cada grupo.

1.5.6. Protocolos No ruteables

A principios y mediados de 1990s, una de las razones por las que Cisco vendió muchos ruteadores es porque el IOS podían dirigir más protocolos de capa 3 que la mayoría. Sin embargo, algunos de los protocolos no son ruteables. Para apoyar aquellos, Cisco apoyó y desarrollo variaciones de puenteo para apoyar los protocolos no ruteables. ¿Qué hace que un protocolo sea no ruteable? Básicamente, una pila de protocolo que no define un equivalente de capa 3 de OSI, incluyendo una estructura lógica de direcciones de Capa 3, no puede ser ruteado. Para ser justo, porque la respuesta a la pregunta "¿es un protocolo ruteable?" para cualquier protocolo en particular es más que una discusión, no hay ninguna regla estricta y rápida que gobierne lo que tiene que ser verdad para un protocolo a ser considerado ruteable. Como este capítulo muestra, sin embargo, remitiendo los paquetes (L3PDUs) basado en una dirección de destino equivalente a la capa 3 involucra ruteo, una pila protocolar sin Capa 3 es considerada como no ruteable.

Si un protocolo es no ruteable, entonces el puenteo debe habilitarse para soportar esos protocolos. Para soportar los protocolos no ruteables sobre enlaces WAN, deben usarse algunos otros protocolos, tales como, punteando, encapsulados y switcheo de enlace de datos. Los detalles de cómo soportar los protocolos no ruteables están más allá de nuestro alcance. Lo mejor es conocer los protocolos no ruteables más populares. Considere la tabla 15 que lista los protocolos que algunas personas consideran ser no ruteables:

1.6. Protocolos orientados a conexión Contra los no orientados a Conexión

Los términos, orientado y no orientado a conexión tienen algunas connotaciones relativamente muy conocidas dentro del mundo de los protocolos de red, sin embargo, la connotación típica puede ser un bit desencaminando. Por ejemplo, la mayoría de las personas correlacionan protocolos orientados a conexión confiables o protocolos de recuperación de error porque las dos características se llevan a cabo a menudo por un solo protocolo. Sin embargo, los protocolos orientados a conexión, no tienen que proporcionar la recuperación de error, y los protocolos de recuperación de error no tienen que ser orientados a conexión.

Protocolo orientado a conexión: Es un protocolo cualquiera que requiere un intercambio de mensajes antes de que el traslado de los datos empiece o tiene una correlación preestablecida requerida entre dos puntos finales.

Protocolo no orientado a Conexión: Es un protocolo que no requiere un intercambio de Mensajes y no requiere una correlación preestablecida entre dos puntos finales. Las definiciones son suficientemente generales para que todos los casos puedan cubrirse.

TCP es orientado a conexión porque un juego de tres mensajes debe completarse antes de que los datos se intercambien. Igualmente, SPX es orientado a conexión.
Cuando se usan PVC's En Frame Relay no requiere de ningún mensaje que sea enviado por delante, pero requiere la predefinición en los switches Frame Relay, mientras se establece una conexión entre

dos dispositivos Frame Relay conectados. Los PVC's en ATM también son orientados a conexión, por razones similares.
Como se menciono antes, los protocolos orientados a conexión se asumen a menudo para realizar también la recuperación de error. Sin embargo, Frame Relay y ATM son dos ejemplos en que los protocolos son orientados a conexión pero el protocolo no proporciona la recuperación de error. La tabla 6 proporciona algunos protocolos de ejemplo y dice si ellos son orientados a conexión y recuperación de error.

Tabla 6 Características de los protocolos: Recuperación de error y conexiones

Conectado?	Fiable?	Ejemplos
Orientado a conexión	Si	LLC tipo 2 (802.2), TCP (TCP/IP), SPX (NetWare), X.25
Orientado a conexión	Si	Circuitos virtuales Frame Relay, conexiones virtuales ATM, PPP
No orientado a conexión	Si	TFTP, NetWare NCP (sin ráfaga de paquete)
No orientado a conexión	No	UDP, IP, IPX, AppleTalk DDP, la mayoría protocolos de capa 3, 802.3, 802.5

La opción más típica para un protocolo es ser no orientado a conexión y no realizar la recuperación de error, o ser orientado a conexión y también realizar la recuperación de error. De hecho, muchos protocolos orientados a conexión intercambian la información importante para la recuperación de error cuando la conexión se establece.

Cualquier cabecera con un Frame Check Sequence (chequeo de secuencia de trama - FCS) o campo similar puede usarse para descubrir los errores de bit en el PDU. La detección de error usa el FCS para descubrir el error que se produce desechando el PDU. Sin embargo, la recuperación de error implica que el protocolo reacciona a los datos perdidos y de algún modo causa que los datos sean retransmitidos.

Los siguientes puntos describen la actitud de los actuales libros del curso de Cisco en la recuperación de error:

El protocolo implementado en la conexión, define las cabeceras y parte de los usos de estas cabeceras para numerar y reconocer los datos. Por ejemplo, TCP proporciona la recuperación de error y define una cabecera de TCP. Las cabeceras usadas por ese protocolo tienen alguna enumeración y campos de reconocimiento para ambos reconocimientos de datos y avisan cuando ha estado perdido en la transmisión. Los puntos finales que están enviando y recibiendo datos, usan los campos en esta cabecera para identificar esos datos que fueron enviados y significa que esos datos fueron recibidos.

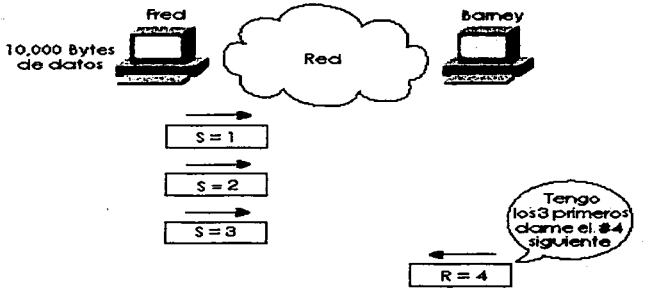
Un transmisor de datos querrá un reconocimiento de los datos. Cuando un error ocurre, muchos algoritmos de recuperación de error le exigen al transmisor que envíe todos los datos, empezando con los datos perdidos. Para limitar el efecto negativo de tener que reenviar muchos datos, se define una ventana de reconocimiento de datos, la cual puede ser dinámica en tamaño. Esta ventana define la cantidad máxima de datos que pueden ser enviados sin conseguir un reconocimiento

1.6.1. Cómo se cumple la recuperación de Error

Sin tener en cuenta cual especificación del protocolo realiza la recuperación de error, todos trabajan básicamente de la misma manera. Genéricamente, los datos transmitidos son etiquetados o numerados. Después del acuse de recibo, las señales del receptor regresan al remitente del cual

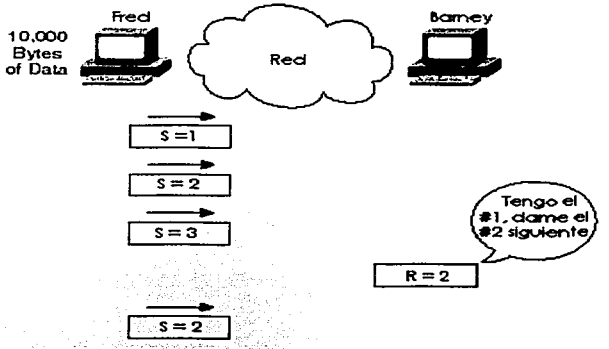
los datos fueron recibidos, usando la misma etiqueta o numero para identificar los datos. La figura 11 resume el funcionamiento.

Figura 11 Reconocimiento adelantado



Como se ilustra en la figura 11, los datos son numerados, como se muestra con los números 1, 2, y 3. Estos números se ponen en la cabecera usada por ese protocolo en particular; por ejemplo, la cabecera de TCP contiene los campos de la enumeración similares. Cuando Barney envía su próxima trama a Fred, Barney reconoce que todas esas tres tramas se recibieron, poniendo su campo de reconocimiento en 4.

Figura 12 Ejemplo de recuperación



El número 4 se refiere a los próximos datos en ser recibidos que se llaman reconocimiento adelantado. Esto significa que el número de reconocimiento en la cabecera identifica los próximos datos que serán recibidos, no el último recibido. (En este caso, 4 es el próximo a ser recibido.)

¿Porque Barney está esperando el próximo paquete número 2?, ¿Qué podría Fred hacer? Existen dos opciones. Fred podría enviar el numero 2 y 3 de nuevo, o Fred podría enviar el número 2 y esperar, esperando que el próximo reconocimiento de Barney dirá 4, indicando que Barney simplemente obtuvo el número 2 y ya tenía antes el número 3.

Finalmente, la recuperación de error usa dos juegos de contadores típicamente: uno para contar los datos en una dirección, y otro para contar los datos en la dirección opuesta. Así, cuando Barney reconoce el número del paquete 2 con el número del campo reconocido en la cabecera, la cabecera también tendría un número de campo enviado que identifica los datos en el paquete de Barney. Por ejemplo, asume en la figura 12 que el paquete anterior que Barney había enviado, era el número 5. El paquete mostrado en la figura sería etiquetado como 6. La tabla 7 resume los conceptos detrás de la recuperación de error y lista la conducta de tres protocolos populares de recuperación de error.

Tabla 7 Ejemplos de recuperación de error, protocolos y sus tramas

Característica	TCP	SPX	LLC2
¿Reconoce los datos en ambas direcciones?	Si	Si	Si
¿Usa el reconocimiento adelantado?	Si	Si	Si
¿Cuenta Bytes o tramas/paquetes?	Bytes	Paquetes	Tramas
¿Es necesario el reenvío de todos los datos, o solo uno parte y esperar el reenvío?	Uno y esperar	Reenviar todo	Reenviar todo

1.6.2. El control de flujo

El control de flujo es el proceso de controlar la tasa a la que una computadora envía los datos. Dependiendo del protocolo en particular, ambos el remitente y el receptor de datos (así como cualquier ruteador, puentes, o interruptores intermedios) podría participar en el proceso de controlar el flujo del remitente al receptor.

El mando de flujo se necesita porque los datos se desechan cuando ocurre la congestión. Un remitente de datos podría estar enviando los datos más rápido de lo que el receptor puede recibir los datos, entonces el receptor desecharía los datos.
También, el remitente podría estar enviando los datos más rápido que el dispositivo de switcheo intermedio (switches y ruteadores) puede remitir los datos, o también causar los desechos. Los paquetes también pueden perderse debido a los errores de la transmisión. Esto pasa en cada red, a veces temporalmente y a veces regularmente, dependiendo de la red y los patrones de tráfico. La computadora receptora puede tener espacio insuficiente en el búfer para recibir la próxima trama entrante, o posiblemente el CPU está demasiado ocupado para procesar la trama entrante. Los ruteadores intermedios podrían necesitar desechar los paquetes basados en la falta temporal de búfer o también de procesamiento.

El control de flujo intenta reducir el innecesario desecho de datos. Comparando los flujos cuando el control de flujo se usa, y cuando no se usa, es útil para entender por qué el control de flujo puede ser útil. Sin el control de flujo, algunos PDUs son desechados. Si algún protocolo fiable en uso ocurre para llevar a cabo la recuperación de error, entonces los datos se reenvían. El remitente sigue enviando tan rápido como le es posible. Con el control de flujo, el remitente puede ser retardado lo suficiente para que el PDU original pueda remitirse a la computadora receptora, y la computadora receptora puede procesar el PDU. Los protocolos de control de flujo no previenen la pérdida de datos debido a la congestión; estos protocolos reducen la cantidad de datos perdidos que a su vez reducen la cantidad de tráfico retransmitido, que esperanzadamente reduce la congestión global.

Sin embargo, con el control de flujo, el remitente se retarda artificialmente o es ahogado para que envíe los datos rápidamente que pudo sin el mando de flujo.
Se requiere estar familiarizado con tres características, o métodos, de implementar el control de flujo:

- Almacenamiento en el bufer
- Anulación de Congestión
- Ventaneo

1.6.3. Almacenamiento en el búfer (Buffering)

Buffering simplemente significa que las computadoras reserven suficiente espacio en el búfer para que las ráfagas de datos entrantes puedan ser sostenidas para su proceso. Ningún esfuerzo hace realmente lenta la tasa de transmisión del remitente de los datos. De hecho, buffering es un método común de tratar con los cambios en la tasa de llegada de los datos que la mayoría de nosotros probablemente asumiría simplemente lo que esta pasando.

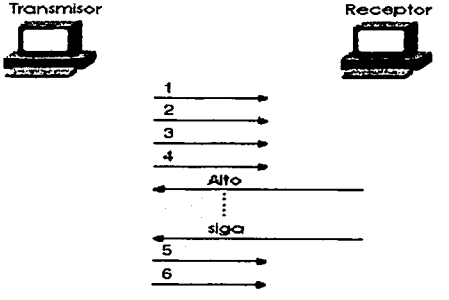
1.6.4. La Anulación de congestión

La anulación de congestión es el segundo método de control de flujo cubierto aquí. La computadora que esta recibiendo los avisos de los datos, de que sus búfers se están llenando. Esto causa o un PDU separado, o un campo en una cabecera, para ser enviado hacia el remitente, señalizando al remitente para dejar de transmitir. La figura 13 muestra un ejemplo.

"Dese prisa y espere" es una expresión popular usada para describir el proceso en este ejemplo de anulación de congestión. Este proceso se usa por los protocolos de enlace de datos seriales como el Control de Enlace de Datos Síncrono (Synchronous Data Link Control - SDLC) y el Procedimiento de Acceso de enlace balanceado (Link Access Procedure Balanced - LAPB)

Un método preferido podría ser conseguir que remitente simplemente reduzca la velocidad en lugar de detener la transmisión. Este método todavía sería considerado como anulación de congestión, pero en lugar de la señalización del remitente para detenerse, la señal significaría la reducción de la velocidad. Un ejemplo es el mensaje del Protocolo de Control de Mensajes de Internet (Internet Control Message Protocol - ICMP) de TCP/IP

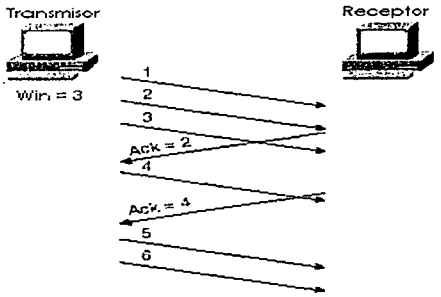
Figura 13 Control de flujo con anulación de congestión



1.6.5. Ventaneo

La tercera categoría de métodos de control de flujo, se llama ventaneo. Una ventana es la cantidad máxima de datos que el remitente puede enviar sin conseguir un reconocimiento. Si ningún reconocimiento se recibe cuando la ventana está llena, entonces el remitente debe esperar por el reconocimiento. La figura 14 muestra un ejemplo. Las líneas sesgadas indican la diferencia de tiempo entre enviar un PDU y su acuse de recibo.

Figura 14 Control de flujo tipo ventaneo



En este ejemplo, el remitente tiene una ventana de tres tramas. Después de que el receptor reconoce el acuse de recibo la trama 1, la trama 4 puede enviarse. Después de un lapso de tiempo, el reconocimiento para las tramas 2 y 3 son recibidas, lo que significa por la trama enviada por el receptor con el campo de reconocimiento igual a 4. Así que, el remitente es libre para enviar dos tramas más. (Tramas 5 y 6) antes de que otro reconocimiento se reciba.

1.6.6. Resumen de control de flujo

La tabla 11 resume las condiciones del control de flujo y proporciona ejemplos de cada tipo. Memorizando estas condiciones deben ayudar a su memoria acerca de los conceptos del control de flujo.

Tabla 11

Nombre Usado en Este Libro	Otros Nombres	Ejemplo de Protocolos
Bufering	N/A	N/A
Anulación de congestión	Alto/inicio, RNR, Fuente Apaga	SDLC, LAPB, LLC2
Ventaneo	N/A	TCP, SPX, LLC2,

Capitulo 2 Redes Lan, Wan y Protocolos de Red

2.1. Introducción

2.1.1. Switcheo LAN

Un switch Ethernet parece usar la misma lógica que un puente transparente. Sin embargo, la lógica interior del switch se optimiza para realizar la función básica de escoger cuándo remitir y cuándo filtrar una trama. Así como con un puente transparente, la lógica básica de un switch LAN es como sigue:

Paso 1 Se recibe una trama

Paso 2 Si el destino es una transmisión o multicast, remitir en todos los puertos.

Paso 3 Si el destino es un unicast y la dirección no está en la tabla de direcciones, remitir en todos los puertos.

Paso 4 Si el destino es un unicast y la dirección está en la tabla de direcciones, remite la trama fuera del puerto asociado, a menos que la dirección MAC este asociada con el puerto entrante.

2.1.2. Puenteo transparente

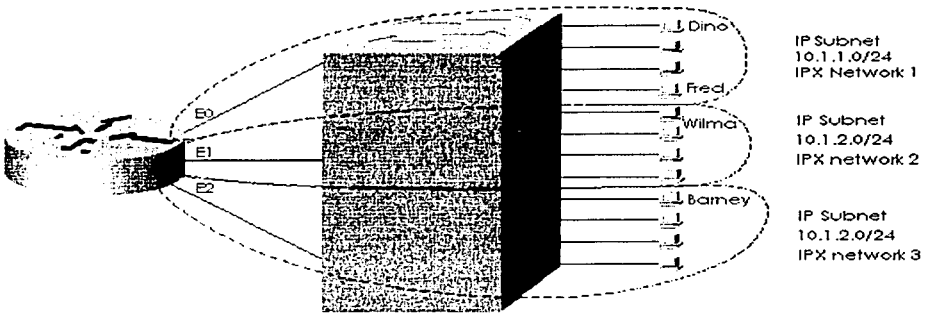
Se le llama transparente porque los dispositivos del punto final no necesitan saber que existe(n) puente(s). En otros términos, las computadoras en la LAN no se comportan diferentes en la presencia o ausencia de puentes transparentes. El puenteo transparente es el proceso de remitir las tramas, cuando sea apropiado. Para lograr esto, los puentes transparentes realizan tres funciones claves:

- Aprender las direcciones MAC examinando las direcciones MAC fuente de cada trama recibida por el puente
- Decidir cuando remitir una trama y cuando filtrar una trama, basado en el destino de las direcciones MAC
- Creando un ambiente de lazo libre con otros puentes que usan el Protocolo de árbol de expansión

2.2 LANs virtuales

Una LAN virtual (VLAN) es un dominio de transmisión creado por uno o más switches. La VLAN se crea por medio de la configuración en el switch. Si un diseño requiere tres dominios de transmisión separados, podrían ser usados tres switches para cada dominio de la transmisión. Cada switch también se conectaría a un ruteador para que los paquetes puedan rutearse entre los dominios de transmisión. En cambio, usando VLANs, podría usarse un switch el cual manejaría tres juegos diferentes de puertos así como también tres dominios diferentes de transmisión.

Figura 2.1 Ejemplo con tres dominios de transmisión, tres VLANs



El switch en la figura 2.1 remite las tramas a las interfaces del ruteador sólo si la trama es una transmisión o se destina para una de las direcciones MAC del ruteador. Por ejemplo, Fred envía las tramas a la dirección MAC E0 del ruteador cuando intenta comunicarse con Barney; esto es porque el ruteador predefinido de Fred debe ser la dirección IP de la interfase E0 del ruteador. Sin embargo, cuando Fred envía las tramas a Dino, la dirección MAC de destino de la trama es la dirección MAC de Dino, y no hay necesidad que el interruptor involucre al ruteador. Las transmisiones enviadas por Fred no van a la otra VLAN porque cada VLAN es un dominio de transmisión por separado.

Las VLAN nos permiten movimientos fáciles, incorporaciones, y cambios. Por ejemplo, si Barney se mudara a una oficina diferente, la cual se conectase a un puerto diferente en el switch, todavía se puede configurar para estar en la VLAN. No es necesario ningún cambio en la dirección de la Capa 3, lo que significa que no se necesitan hacer cambios en Barney.

Pueden obtenerse muchos beneficios de las VLAN, incluyendo éstas:

- Con las VLANs, movimientos, sumas, y cambios en las conexiones de los dispositivos son más fáciles.
- Obligando al dispositivo de ruteo de capa 3 a involucrarse entre VLANs, el mando de control administrativo mayor puede usarse (mejor conteo, listas de acceso, y así sucesivamente).
- El consumo innecesario del ancho de banda LAN es reducido comparado con un solo dominio de transmisión.
- El uso innecesario del CPU es reducido por el resultado de la reducción de la transmisión remitida.

2.2.1. Numerando los puertos (Interfaces)

Los términos interfase y puerto (port), se usan para describir los conectores físicos en el hardware del switch. Por ejemplo, el comando **show running-config** usa el término interfase; el comando **show spantree** usa el término port.

2.2.2. Configuración Básica de IP y Puerto Dúplex

Dos características comúnmente configuradas inmediatamente durante la instalación del switch son soporte para TCP/IP y el establecimiento dúplex en los puertos claves del switch. Los switches soportan IP, pero de una manera muy diferente que con un ruteador. El switch actúa más como un host IP, con una sola dirección/mascara para el switch y un ruteador predefinido. Cada puerto/interfase no necesita una dirección IP porque el switch no está realizando el ruteo de la capa 3. De hecho, si no hubiera ninguna necesidad de manejar el switch, no se necesitaría IP en el switch en lo absoluto.

La segunda característica típicamente configurada al momento de la instalación es la preconfiguración de algunos puertos para siempre usar half o full duplex en lugar de permitir la negociación. A veces, la autonegociacion puede producir resultados imprevisibles. Por ejemplo, si un dispositivo conectado al switch no soporta la autonegociacion, el switch Catalyst establece el correspondiente puerto del switch al modo half-duplex predeterminadamente. Si el dispositivo conectado se configura para full duplex, ocurrirán errores de colisión más tarde en el full duplex del extremo. Para evitar esta situación, se establecen manualmente los parámetros duplex del switch para comparar el dispositivo conectado cuando el soporte para la autonegociación está en cuestión.

2.3. Protocolos de red

2.3.1. Protocolos TCP/IP

Cuando se trabaja con múltiples protocolos a diario; ninguno de éstos es más importante que TCP/IP. TCP y UDP son los dos protocolos de la capa de transporte (capa 4) más usados a menudo por las aplicaciones en una red TCP/IP. ICMP y ARP son de hecho, parte de la capa de red (capa 3) de TCP/IP y se usa junto con IP.

2.3.1.1. Protocolo de Control de Transmisión (TCP)

Una característica común del ruteo, es desechar paquetes por una variedad de razones. Por ejemplo, el paquete no podía encontrar la ruta, o no había suficiente espacio en el búfer del ruteador para guardar el paquete hasta que el próximo enlace estuviese disponible. Los protocolos de capa 3 no proveen típicamente la retransmisión.

Este protocolo popular de capa más alta lleva a cabo la recuperación de error, llamado Protocolo de Control de Transmisión (Transmision Control Protocol - TCP). Definido en RFC 793, TCP realiza la recuperación del error así como otras características, incluyendo estas:

- Transferencia de datos
- Multiplexaje
- Recuperación de error (fiabilidad)
- Control de Flujo usando ventaneo
- Establecimiento de Conexión y terminación

TCP logra estas metas a través de los mecanismos de las computadoras en los extremos finales. TCP confía en IP para la entrega de extremo a extremo de los datos, incluyendo los problemas de ruteo. En otros términos, TCP realiza sólo parte de las funciones necesarias para entregar los datos entre las aplicaciones.

2.3.1.1.1. Transferencia de Datos Pedidos

Como con otras funciones en cualquier pila protocolar, TCP provee servicio para la siguiente capa más alta. La pila del protocolo TCP/IP tiene sólo cuatro capas; esto es, para que la capa siguiente más alta de TCP sea la capa de aplicación. Por consiguiente, el traslado de datos TCP implica la entrega de datos de una aplicación a otra. (La capa de aplicación TCP/IP realiza las funciones similares a las tres capas superiores del modelo OSI.) Las aplicaciones usan los servicios TCP emitiendo las llamadas programáticas a TCP, proporcionando los datos a ser enviados, el destino la dirección de destino IP, y un número de puerto que identifica la aplicación que debe recibir los datos. El número del puerto, junto con la dirección de destino IP y el nombre del protocolo de capa de transporte (TCP), forman un enchufe.

TCP logra que los datos se transfieran estableciendo una conexión entre un enchufe en cada una de las computadoras finales. Las aplicaciones usan los servicios TCP abriendo un enchufe; TCP maneja la entrega de los datos al otro enchufe. Un enchufe par fuente/destino únicamente identifica una relación entre las dos aplicaciones en una red. TCP maneja el traslado pedido de datos entre estos dos enchufes, usando los servicios IP para la entrega de los datos

2.3.1.1.2. Multiplexaje

El multiplexaje se refiere a las opciones hechas en la recepción de los datos. La tarea del multiplexaje TCP, es decidir a cuál proceso de la capa de aplicación darle los datos, después de que los datos se reciben.

2.3.1.1.3. Recuperación de Error (Fiabilidad)

El traslado fiable de los datos es una de las características más importantes y típicamente más recordadas de TCP. Para lograr la fiabilidad, se numeran los bytes de los datos usando los campos de secuencia y reconocimiento en la cabecera TCP. TCP logra la fiabilidad en ambas direcciones, mientras que, usando el campo de numeración de secuencia en una dirección combinado con el campo de reconocimiento en la dirección opuesta.

2.3.1.1.4. Control de flujo Usando ventaneo

TCP lleva a cabo el control de flujo tomando ventaja de los campos de secuencia y reconocimiento en la cabecera TCP, junto con otro campo llamado "campo de ventaneo". Este campo de ventana implica el número máximo de bytes sin reconocimiento pendientes a cualquier instante a tiempo. La ventana empieza pequeña y entonces crece hasta que los errores ocurran. La ventana entonces se desliza de arriba abajo basado en el desempeño de la red. Cuando la ventana está llena, el transmisor no enviará, el cual controla el flujo de datos.

2.3.1.1.5. El Establecimiento de la Conexión y Terminación

Ocurre antes de que cualquiera de las otras características de TCP puedan empezar su trabajo. El establecimiento de la conexión se refiere al proceso de inicializar la secuencia y los campos de reconocimiento y acordando los números de los puertos usados.

2.3.1.2. Protocolo de Datagrama de Usuario (UDP)

UDP fue diseñado para proveer un servicio para aplicaciones en las cuales podrían intercambiarse mensajes TCP. UDP no proporciona ninguna fiabilidad, ningún ventaneo, y ninguna función para asegurarse de que los datos se reciben en el mismo orden en el cual fueron enviados. Sin embargo, UDP proporciona algunas funciones de TCP, como la transferencia de datos y multiplexaje, y lo hace con menos bytes de cabecera adicional en la cabecera UDP.

El multiplexaje UDP usa los números de puerto de la forma en que lo hace TCP. La única diferencia en UDP (comparado con TCP) es que los enchufes, en lugar de designar TCP como el protocolo de transporte, el protocolo de transporte es UDP. Una aplicación podría abrir los números del puerto idénticos en el mismo host pero usando TCP en un caso y UDP en el otro. Esto no es típico pero ciertamente se permite. Servidores que permiten uso de TCP y UDP reservan el uso del mismo número del puerto para cada uno

La transferencia de datos UDP difiere de TCP en la transferencia de datos, no se vuelven a pedir los datos ni se cumple la recuperación. Aplicaciones que usan UDP son tolerantes a la perdida de datos, o ellos tienen algún mecanismo de aplicación para recuperar los datos perdidos.

2.3.1.3. Protocolo de resolución de dirección (ARP)

Un problema con el que se tiene que lidiar a menudo es el siguiente: ¿Dada una dirección de capa 3, cual es la dirección de la capa 2 correspondiente? El protocolo de resolución de dirección (Address Resolution Protocol - ARP) es el proceso por el cual esta pregunta se responde por un host IP en una LAN.

ARP es necesario, ya que para enviar un paquete IP por alguna LAN, la cabecera de enlace de datos y su *trailer* (el cual encapsula el paquete) debe crearse primero. La dirección MAC fuente en esta nueva cabecera es conocida, pero el destino MAC no es de antemano conocido; ARP es el método IP usado para descubrir la dirección MAC de destino.

2.3.1.4. Protocolo de mensaje de control de Internet (ICMP)

El Protocolo de mensaje de control de Internet I(Internet Control Message Protocol - ICMP) ayuda al control y el manejo de trabajo IP y por consiguiente se considera que es parte de la capa de red de TCP/IP. RFC 792 define a ICMP e incluye la siguiente cita, la cual describe bien el protocolo:

Ocasionalmente una pasarela (gateway) o host de destino se comunicará con un host fuente, por ejemplo, para informar un error en el proceso del datagrama. Para tales propósitos se usa el Protocolo de Mensaje de Control de Internet (ICMP). ICMP usa el soporte básico IP como si fuera un protocolo de alto nivel; sin embargo, ICMP realmente es parte íntegra de IP, y debe llevarse a cabo por cada módulo IP. Varios mensajes ICMP están en uso incluso en la red IP más pequeña.

2.3.1.5. FTP y TFTP

El Protocolo de Traslado de archivo (File Transfer Protocol - FTP) y el Protocolo de Traslado de Archivo Trivial (Trivial File Transfer Protocol - TFTP) son dos protocolos de transferencia de archivos popularmente usados en una red IP típica. La mayoría de los usuarios usa FTP, considerando el ruteador y los administradores de switches usan TFTP. Cual es "mejor" depende parcialmente de lo que está haciéndose. Una pregunta más importante puede ser típicamente, "¿Cual se apoya en los dispositivos que necesitan transferir el archivo?" Dada una opción hoy, la mayoría de los usuarios escogerá FTP porque tiene muchas más características robustas. TFTP es el favorito de los administradores de ruteadores, ya que el IOS no soporta FTP como una aplicación.

2.3.1.5.1. FTP

FTP es una aplicación basada en TCP, la cual tiene muchas opciones y características, incluyendo las capacidades para cambiar los directorios, lista de archivos usando una variedad de juegos de caracteres, transfiere archivos múltiples con un solo comando, y usa una variedad de juegos de caracteres o formatos de archivo. Más importante en este contexto, es el funcionamiento básico de FTP.

2.3.1.5.2. TFTP

El Protocolo de Transferencia de Archivo trivial (TFTP) es una aplicación basada en UDP con características muy básicas. Una de las razones por la que semejante aplicación se necesita es que TFTP toma un poco de memoria para cargar y toma un poco de tiempo para programar. Con la llegada de memoria cada vez más económica y mejor procesamiento, tales ventajas parecen triviales. Hablando prácticamente, si se piensa frecuentemente en transferir los archivos de su PC, FTP probablemente es lo que se usará. Sin embargo, para transferir los archivos dentro y fuera de ruteadores y switches basados en el IOS, Cisco soporta TFTP, no FTP.

TFTP usa UDP, así que no hay ningún establecimiento de conexión y ninguna recuperación de error por la capa de transporte. Sin embargo, TFTP usa la recuperación de capa de aplicación empotrando una pequeña cabecera entre la cabecera UDP y los datos. Esta cabecera incluye los códigos para el caso de, leer, escribir, y reconocimiento con un esquema numerado que numera los 512 bloques de bytes de datos. Estos números de bloques se usan para el recibo de reconocimiento y el reenvío de datos. TFTP envía un bloque y espera un reconocimiento antes de enviar otro bloque, esencialmente el equivalente al tamaño de una ventana de 1.

2.4. Direccionamiento privado

Existe una necesidad legítima por la cual las direcciones IP que nunca se usarán en las redes IP interconectadas, llamadas Internet. Así que, al diseñar el direccionamiento IP de semejante red, una organización podría escoger cualquier número de red(es) que quiera, y todas funcionarían bien, hasta que la organización decida conectarse a la Internet.

Cuando se necesitan direcciones IP que no estén conectadas a la Internet, pueden extraerse de un juego de redes IP, llamadas Internets privadas.

En otros términos, cualquier organización puede usar éstos números de red. Sin embargo, a ninguna organización se le permite anunciar estas redes como rutas en la Internet. El espacio de dirección de la versión 4 de IP se conserva si todas las organizaciones usan las direcciones privadas en los casos para los que nunca habrá una necesidad de una conectividad en Internet.

El requisito del direccionamiento privado en el cual los host privadamente direccionados no pueden comunicarse con otros a través de la Internet, puede ser una restricción particularmente molesta. La solución: el direccionamiento privado con el uso de la Traducción de Dirección de Red (Network Address Translation - NAT)

2.4.1. Traducción de las direcciones de la red

La traducción de las direcciones de red (Network Address Translation - NAT) es una función definida implementada en el IOS que permite a un host que no tiene una dirección IP valida registrada, comunicarse con otros host a través de la Internet. Los host pueden estar usando direcciones privadas o direcciones asignadas a otra organización; en cualquier caso, NAT permite que estas direcciones que no están listas para Internet, continúen siendo usadas, pero que sigan permitiendo la comunicación con los host a través de la Internet.
NAT logra su meta usando una dirección válida en alguna red IP registrada para representar la dirección inválida al resto de la Internet. La función NAT cambia las direcciones IP como sea necesario dentro de cada paquete IP. NAT también puede usarse cuando la organización privada no está usando el direccionamiento privado, pero en cambio, este usando un número de red registrado a nombre de otra compañía.

2.4.2. Direccionamiento IPX y ruteo

La pila del protocolo NetWare de Novell define el intercambio de paquetes de Internet (Internetwork Packet Exchange - IPX) como un protocolo equivalente a la capa de red, como se aprecia en la figura 2.1, IPX será el enfoque de esta sección inicial.

IPX define la estructura de dirección de 80 bits la cual usa una parte de red de 32 bits y una parte de nodo de 48 bits. Como con IP y AppleTalk, todas las interfaces anexas al mismo enlace de datos usan direcciones en la misma red. La tabla 2.1 lista cuatro características del direccionamiento IPX. Las características listadas en la tabla 2.1 so las mismas características para describir genéricamente el bien diseñando esquema de direccionamiento de la capa 3.

Figura 2.1 Protocolos Novell NetWare

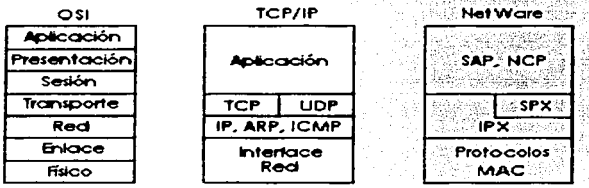


Tabla 2.1 Detalles del direccionamiento IPX

Característica	**Descripción**
Tamaño de un grupo	Las direcciones IPX usan una parte de nodo de 48 bits de la dirección, dando 248 posibles direcciones por red (menos unos cuantos valores reservados) la cual debe ser lo suficientemente grande.
Direcciones únicas	IPX requiere que las direcciones LAN MAC sean usadas como la parte del nodo de la dirección IPX. Esto permite la asignación fácil y la poca probabilidad de duplicación. Asegurar que no se hace ninguna duplicación de los números de red, es la preocupación más grande, cuando se configuran los números de red.
Agrupamiento	El concepto de la agrupación es idéntico a IP, con todas las interfaces anexas al mismo medio usando el mismo número de red. No hay ningún equivalente de subnetting IP.
Asignando direcciones dinámicas	Las direcciones IPX de cliente, son dramáticamente asignadas como parte de las especificaciones del protocolo. Se configuran servidores y ruteadores con el número(s) de red en sus interfaces físicas. Los servidores pueden escoger generar un número de red interior automáticamente al momento de la instalación.

2.5. Protocolos de Ruteo

La lógica de vector de distancia es la lógica usada por el Protocolo de Información de Ruteo (Routing Information Protocol - RIP) y por el Protocolo de Ruteo de Entrada Interior (Interior Gateway Routing Protocol - IGRP), así como de IP RIP. De hecho, algunos conceptos del vector de distancia, incluso se aplican al Protocolo de Anuncio de Servicio NetWare (Service Advertising Protocol - SAP), aunque SAP no distribuya la información de ruteo.

2.5.1. Protocolos de Ruteo de Vector de Distancia

El primer término que necesita ser definido es protocolo de ruteo. Este término puede contrastarse con protocolo ruteado. Aquí se muestran dos de sus características que pueden ser útiles:

- Un protocolo de ruteo llena la tabla de ruteo con información de ruteo. Los ejemplos incluyen RIP e IGRP.
- Un protocolo ruteado es un protocolo que tiene una especificación equivalente en la capa 3 de OSI, la cual define direccionamiento lógico y ruteo. Los paquetes definidos por la capa de red (capa 3) la porción de estos protocolos puede rutearse. Ejemplos de protocolos incluyen a IP e IPX.

Los protocolos de ruteo IP llenan la tabla de ruteo IP con rutas válidas libres de vueltas, (afortunadamente). El vector de distancia de los protocolos de ruteo tiene muchas características que previenen las vueltas. Cada ruta incluye un número de subred, la interfase de salida, la cual remite los paquetes para que estos se entreguen a esa subred, y las direcciones IP del próximo ruteador que debe recibir los paquetes destinados para esa subred (si es necesario). Una analogía para el ruteo, es el proceso en el cual una persona haría un viaje hacia alguna parte en la que nunca ha estado, la cual podría buscar señales en el camino refiriéndose a la ciudad de destino, indicándole que tiene que tomar la próxima desviación. Repitiendo el proceso en cada intersección hasta la ciudad correcta.
En caso de que ocurra una vuelta de ruteo y que nunca pregunte cuál es la dirección a seguir, esta persona podría dar vueltas para siempre, o por lo menos hasta que se le acabe la gasolina.

Las metas documentadas en la lista siguiente son comunes para cualquier protocolo de ruteo IP, sin tener en cuenta su tipo de lógica subyacente:

- Para aprender dinámicamente y llenar la tabla de ruteo de una ruta a todas las subredes en la red.
- Si más de una ruta hacia una subred está disponible, para poner la mejor ruta en la tabla de ruteo.
- Para notar cuando las rutas en la tabla ya no son válidas, y para quitar esas rutas de la tabla de ruteo.
- Si una ruta es removida de la tabla de ruteo y está disponible otra ruta a través de otro ruteador vecino, agregar la ruta a la tabla de ruteo.
- Para agregar las nuevas rutas, o reemplazar las rutas perdidas con la mejor ruta actualmente disponible, tan rápidamente como sea posible. El tiempo entre perder la ruta y encontrar una ruta de reemplazo activa, se llama tiempo de convergencia.
- Para prevenir las vueltas de ruteo.

2.5.2. Comparando los Protocolos de Ruteo

Existen varios protocolos de ruteo para TCP/IP. La larga historia de IP y su continua popularidad han requerido la especificación y creación de varias opciones. Así que, es útil clasificar los protocolos de ruteo IP basándose en sus diferencias.

Una mayor clasificación de los protocolos de ruteo IP, es si ellos están optimizados para crear las rutas dentro de una organización o rutas entre dos o más organizaciones interconectadas. Los protocolos de ruteo exteriores están optimizados para usarse entre ruteadores de diferentes organizaciones. El Protocolo de Entrada de la frontera (Border Gateway Protocol - BGP) y el Protocolo de la Entrada Exterior (Exterior Gateway Protocol - EGP) son las dos opciones para los protocolos de ruteo exteriores; BGP es el más popular y el más desarrollado recientemente de los dos. (EGP no es técnicamente un protocolo de ruteo; está obsoleto.)

El termino protocolo de ruteo es el término usado para describir los programas y procesos usados para intercambiar y aprender información de ruteo. Otros documentos llaman a estos mismos programas y procesos "algoritmos de ruteo".

2.5.3. Ruteo de vector de distancia

Los especialistas en redes trabajan a diario con problemas de ruteo; algunos de estos problemas son resultado de la lógica detrás del vector de distancia que los protocolos de ruteo. Para entender que significa el vector de distancia se necesita entender como un protocolo de ruteo logra sus siguientes metas:

- Aprender información de ruteo
- Notificar rutas fallidas
- Agregar las mejores rutas actuales después de que una ha fallado
- Prevenir las vueltas

La siguiente lista resume la conducta de un ruteador que usa el RIP-1 o los protocolos de ruteo de vector de distancia IGRP:

- Subredes conectadas directamente son ya conocidas por el ruteador; estas rutas se anuncian a los ruteadores vecinos.
- Actualizaciones de ruteo son broadcast (o en muchos casos, multicast). Esto es para que todos los ruteadores vecinos puedan aprender las rutas vía transmisión única o actualización multicast.
- Actualizaciones de ruteo se escuchan para que este ruteador pueda aprender las nuevas rutas.
- Una métrica describe cada ruta en la actualización. La métrica describe que tan buena es la ruta; si las rutas múltiples hacia la misma subred son aprendidas, la ruta más baja métrica se usa.
- La información de la Topología en las actualizaciones de ruteo como mínimo, la subred y la información métrica
- Se esperan actualizaciones periódicas para ser recibidas de ruteadores vecinas en un intervalo especifico
- Una ruta aprendida de ruteadores vecinos se asume estar en ese ruteador
- Se asume que una ruta aprendida de un ruteador vecino ha terminado en ese ruteador.

- Una ruta fallida se anuncia durante un tiempo, con una métrica la cual implica que la red es de distancia infinita. Esta ruta es considerada inutilizable. La infinidad se define por cada protocolo de ruteo para que algún valor métrico sea muy grande. Por ejemplo, la métrica infinita de RIP es 16 porque el máximo valor de RIP es 15.

2.5.4. El Horizonte dividido, Holddown, y Envenenamiento de la Ruta

Las vueltas de ruteo pueden ocurrir al usar protocolos de ruteo de vector de distancia, ya que la mala información de ruteo puede propagarse. El horizonte partido es una solución muy popular al problema y funciona muy bien en la mayoría de las topologías.

2.5.5. RIP e IGRP

RIP e IGRP usan la lógica de vector de distancia, así que son muy similares, pero existen unas cuantas diferencias mayores. La tabla 2.2 muestra las características de RIP e IGRP.

Tabla 2.2 RIP e IGRP Característica de comparación

Característica	**RIP (Predeterminadas)**	**IGRP (Predeterminadas)**
Tiempo de actualización	30 segundos	90 segundos
Métrica	Cuenta de salto	La función de Ancho de banda y retraso (valor predeterminado); puede incluir fiabilidad, carga, y MTU
Tiempo de espera	180	280
Actualizaciones (disparadas) flash	Si	Si
Mascara enviada en actualización	No para RIP v1; si para RIP v2	No
Valor de la métrica infinito	16	4,294,967,295

La métrica con IGRP es más robusta que la métrica de RIP. La métrica es calculada usando el ancho de banda y retrasando las configuraciones en la interfase en que la actualización fue recibida. Usando el ancho de banda y el retraso, la métrica es más significativa; las rutas de salto más largas sobre los enlaces más rápidos, pueden ser consideradas rutas buenas. La métrica usada por RIP IP es cuenta de salto. Cuando una actualización se recibe, la métrica para cada subred en la actualización significa que el número de ruteadores entre el ruteador que recibe la actualización y cada subred. Antes de enviar una actualización, un ruteador incrementa su métrica para las rutas hacia cada subred por 1. En otros términos, una actualización de ruteo incluye valores métricos que dicen lo que su métrica debe ser al ruteador receptor.

2.5.6. Resumen de los protocolos de ruteo de vector de distancia

Los protocolos de ruteo de vector de distancia aprenden y anuncian rutas. Las rutas puestas en la tabla de ruteo deben ser libres de vueltas y deben ser las rutas conocidas que funcionen mejor, la métrica se usa para escoger la mejor ruta. Mecanismos tales como el horizonte partido y tiempos de espera se usan para prevenir las vueltas de ruteo.

2.6. Configuración de RIP e IGRP

La tabla 2.3 y 2.4 resumen los comandos más populares usados para, la configuración y verificación de RIP e IGRP. Dos muestras de configuración siguen.

Tabla 2.3 Comandos de configuración IP RIP e IGRP

Comando	Modo de configuración
router rip	Global
router igrp proceso de identificación	Global
network numero de red	Subcomando del ruteador
passive-interface tipo numero	Subcomando del ruteador
maximum-paths x	Subcomando del ruteador
variance multiplicador	Subcomando del ruteador
traffic-share {balanceado | min}	Subcomando del ruteador

Tabla 2.4 IP RIP e IGRP EXEC

Comando	Función
show ip route [subred]	Muestra toda la tabla de ruteo, o una entrada si se introduce subnet
show ip protocol	Muestras los parámetros del protocolo de ruteo y los valores actuales del cronometro
debug ip rip	Emite mensajes log para cada actualización RIP
debug ip igrp transactions	Emite mensajes log con detalles de las actualizaciones IGRP
debug ip igrp events	Emite mensajes log para cada paquete IGRP
Ping	Envía y recibe mensajes de eco ICMP para verificar la conectividad
Trace	Envía una serie de ecos ICMP con valores TTL crecientes para verificar la ruta actual a un host

2.6.1. El comando red (network)

Cada comando network habilita RIP o IGRP en un conjunto de interfaces. El comando network causa la implementación de las siguientes tres funciones:

- Las actualizaciones de ruteo son transmisiones o multitransmisiones fuera de una interfase.
- Las actualizaciones de ruteo son procesadas si ellas entran en esa misma interfase.
- La subred directamente conectada a esa interfase es anunciada.

El comando **network** coincide con algunas de las interfaces en un ruteador. Las interfaces que coincidieron por el comando **network** tienen las tres funciones previamente mencionadas realizadas en ellas. Los ejemplos proporcionan un entendimiento mucho más fácil del comando **network**.

2.6.2. Métrica IGRP

IGRP usa un compuesto métrico, esta métrica es calculada como una función de ancho de banda, retraso, carga, y fiabilidad. Predeterminadamente, se consideran sólo el ancho de banda y el retraso; los otros parámetros sólo son considerados si se habilitan vía configuración. El retraso y el ancho de banda no son los valores moderados pero son establecidos por medio de los subcomandos de la interfase **delay** y **bandwidth**. (La misma fórmula se usa para calcular la métrica

para EIGRP, pero con un factor escalado para que los valores métricos reales sean más grandes, permitiendo más granularidad en la métrica.)

2.6.3. Rutas múltiples hacia la misma subred

Predefinidamente, el IOS soporta cuatro rutas de igual costo hacia la misma subred IP en la tabla de ruteo al mismo tiempo. Este número puede cambiarse entre 1 y 6 usando el subcomando de configuración **ip maximun-paths** del ruteador X, donde X es el número máximo de rutas hacia cualquier subred. Como se menciono antes, los paquetes son balanceados en una dirección base por destino predeterminadamente; los paquetes también pueden ser balanceados en una base paquete por paquete, paro a una penalización del desempeño

La formula métrica usada para IGRP (e EIGRP) propone un problema interesante al considerar las rutas de métrica igual. IGRP puede aprender más de una ruta hacia la misma subred, con la métrica diferente; sin embargo, es muy probable que la métrica nunca sea precisamente igual. El subcomando del ruteador **variance** se usa para definir que tan variables pueden ser las rutas para ser consideradas para tener métricas iguales. El parámetro para el comando (el multiplicador) es multiplicado por la más baja de las métricas recibidas para una subred en particular.
Cualquiera de las rutas con una métrica menor que el producto de veces de la "mejor métrica", el multiplicador es considerado a ser igual.

Algunas torceduras interesantes en la lógica deben considerarse cuando se decide si usar una o múltiples rutas de costo igual con IGRP. Si se establece maximum-paths a 1, entonces la primera de estas rutas de igual costo aprendida para cada subred en la tabla de ruteo. Sin embargo, estas podrían ser las rutas con la métrica más grande. Para evitar eso, podrían tenerse maximum-paths como valor predefinido en 4 o podrían codificarse como algún otro número; además, el comando **variance** puede usarse para definir que tan cercanas deben ser las métricas de valor, para ser consideradas igual. Sin embargo, en ese caso, algo de tráfico fluirá sobres las rutas con la mejor métrica, y algo fluirá sobre la ruta con la peor métrica. Ninguna situación parece ser la óptima.

Una diferente, y posiblemente mejor alternativa, es usar el subcomando **IGRP trafic-share min** en conjunto con los comandos **maximum-paths** y **variance**. Este comando le dice al ruteador que agregue las rutas múltiples a la tabla de ruteo, pero para enviar el tráfico solamente usando la ruta con la métrica más pequeña. Esto permite que todas las rutas hacia cada subred, estar en la tabla de ruteo, la cual es una ventaja para una convergencia más rápida. Sin embargo, todo el tráfico va a través de la ruta de métrica más baja que esta actualmente en la tabla de ruteo. El comando **traffic-share balanced**, el cual es el predefinido, le dice al ruteador que use todas las rutas basadas proporcionalmente en la métrica para cada ruta.

2.7. Configurando el ruteo y mas protocolos de ruteo

El comando **show ip route** tiene un miríada de opciones que serán útiles al arreglar una red grande. El comando **ip show protocol** también puede proporcionar alguna información muy útil al arreglar un problema de ruteo. Con una red pequeña, la mayoría de las opciones en el comando **show ip route** son innecesarias. Sin embargo, sabiendo las opciones y lo que cada uno puede hacer será muy útil para su trabajo con redes más grandes.

2.7.1. IPX RIP, SAP, y GNS

Es importante conocer otros dos protocolos NetWare usados por el ruteador: El Protocolo de Anuncio de Servicio (Service Advertisement Protocol - SAP) y Obtener el Servidor más Cercano (Get Nearest Server - GNS). Ya que IPX RIP e IP RIP fueron originalmente basados en el mismo protocolo (XNS RIP), los dos son muy similares. SAP y GNS no tienen ninguna característica equivalente en

TCP/IP. RIP para IPX trabaja de una manera similar a la de IP RIP. La diferencia más obvia es que IPX RIP anuncia números de red IPX, no números de subred IP. La tabla 2.5 lista las similitudes y diferencias.

Tabla 2.5 Comparación para IPX e IP

Novell RIP	**IP RIP**
Usa vector de distancia	Usa vector de distancia
Está basado en XNS RIP	Está basado en XNS RIP
Usa tiempo de actualización de 60 segundos (predeterminado)	Usa tiempo de actualización de 60 segundos (predeterminado)
Usa conteo de cronometro como métrica primaria, conteo por saltos como métrica secundaria	Usa conteo por saltos como única métrica

IPX RIP usa dos métricas: tic tacs y saltos. Los tic tacs son 1/18 de segundo; la métrica es un contador entero del número de retrasos de tic tacs para esta ruta. Predeterminadamente, un ruteador Cisco trata a un enlace como si tuviera un cierto número de retraso de tic tacs. Las interfaces LAN tienen un tic tac predeterminadamente y las interfaces WAN tienen predeterminadas seis tic tacs. El número de saltos es considerado solo cuando el numero de tic tacs esta atado. Usando los tic tacs como primer métrica, las mejores rutas pueden escogerse en lugar de solamente usar el conteo a pasos. Por ejemplo, una ruta de tres brincos, tres tic tacs que usa tres Ethernets, se escogerá sobre una ruta de dos brincos, ocho titacs, que usa dos Ethernet y un enlace

2.7.2. Protocolo de Anuncio de Servicio

El Protocolo de Anuncio de Servicio (Service Advertisement Protocol - SAP) es una de las partes más importantes de las especificaciones del protocolo NetWare, pero también es uno de los desafíos más grandes al intentar escalar una red IPX SAP se usa por los servidores para propagar la información que escriben sus servicios. Se esperan que los especialistas en redes estén muy familiarizados con SAP y los papeles los ruteadores al remitir la información SAP.

El proceso SAP trabaja mucho mejor que el proceso usado por un protocolo de ruteo de vector de distancia. De hecho, SAP usa un concepto similar al de horizonte partido para detener a un nodo de anunciar la información SAP que aprendió en una interfase con actualizaciones enviadas fuera de esa misma interfase. Cada servidor envía las actualizaciones SAP cada 60 segundos predeterminadamente que incluye la dirección IPX, nombre del servidor, y tipo de servicio. Cualquier otro servidor y ruteador escucha estas actualizaciones pero no remite el(los) paquete(s) SAP. En cambio, la información SAP se agrega a una tabla SAP en el servidor o ruteador; entonces los paquetes se desechan. Cuando ese ruteador o el tiempo SAP del servidor expiran, se envían las nuevas transmisiones SAP. Como con IPX RIP para la información de ruteo, IPX SAP propaga la información de servicio hasta que todos los servidores y ruteadores han aprendido acerca de todos los servidores

2.7.3. Entubado

Entubar es el proceso por el cual un ruteador encapsula un protocolo de capa 3 dentro de otro protocolo (típicamente IP), para el transporte a través de una red hacia otro ruteador. El ruteador receptor des encapsula el paquete, dejando el protocolo original. Cada ruteador intermedio que se usa entre los puntos finales del entubado ignora el protocolo que esta siendo encapsulando.

Se usan tres términos importantes para describir las tres partes de la entidad que se envía entre los dos ruteadores entubados:

- Protocolo pasajero - Este es el protocolo que esta encapsulándose.
- Protocolo de Encapsulamiento - Para identificar el protocolo pasajero, se usa una cabecera adicional. Se puede pensar en esta cabecera adicional como otro lugar para incluir un campo del mismo tipo que el de la capa de enlace de datos, DSAP, o campo del protocolo. La cabecera IP define que una de estas cabeceras de encapsulamiento de protocolo sigue la de IP, y el protocolo del encapsulamiento identifica el tipo de protocolo pasajero de capa 3 que lo sigue.
- Protocolo de transporte - El protocolo de transporte entrega el protocolo pasajero a través de la red. IP es la única opción en el IOS.

Para cada paquete del protocolo encapsulado (pasajero), hay la adicional cabecera de aplicar la cabecera del paquete del protocolo encapsulado (transporte). Agregando más bytes de cabecera adicional, ciertamente se reduce la eficacia. ¿Así por que usar incluso el entubado en primer lugar? Hay varias razones:

- Para permitir que múltiples protocolos fluyan sobre una troncal de protocolo único
- Para superar los problemas de redes discontinuas
- Para permitir las redes privadas virtuales (VPNs)
- Para superar la limitación de algunos protocolos de ruteo con limitaciones métricas máximas bajas
- Para reducir la cantidad de sobre cabeceo de los protocolos de ruteo

La cantidad de "sobrecabeceo" de estos protocolos esta muy reducido, particularmente cuando están en uso redes sin transmisión de multi acceso (non broadcast multi access - NBMA), tales como Frame Relay así que la troncal de la red WAN solo puede seguir siendo IP, y cuando hay solo grupos aislados de los diferentes protocolos de pasajeros, estos protocolos pueden ser remitidos usando el entubado

2.8. Líneas Arrendadas punto a punto

Los protocolos WAN usados en los enlaces seriales punto a punto proporcionan la función básica de la entrega de datos a través de ese enlace. Los protocolos WAN, Procedimiento de Acceso de Enlace balanceado (Link Access Procedure Balanced - LAPB), el Control de Enlace de Datos de Alto Nivel (High-Level Data Link Control - HDLC), y el Protocolo de Punto a Punto (Point to Point Protocol - PPP), tienen las siguientes funciones en común:

- LAPB, HDLC, y PPP proveen la entrega de datos a través de un solo enlace serial punto a punto.
- LAPB, HDLC, y PPP entregan los datos en los enlaces seriales síncronos. (PPP soporta las funciones asíncronas también.)

Los enlaces síncronos, se usan típicamente en lugar de los enlaces asíncronos, entre los ruteadores. Síncrono simplemente significa que hay un tiempo impuesto ordenando el envío y la recepción al final del enlace. Esencialmente, los lados acordando una cierta velocidad, pero ya que es muy caro construir dispositivos que puedan operar verdaderamente la misma velocidad exactamente, los dispositivos ajustan su velocidad para igualarla a la fuente del reloj. Al contrario de los enlaces asíncronos, en los cuales no se envían bits durante los tiempos ociosos, los enlaces de datos síncronos definen las tramas ociosas. Estas tramas no hacen nada más que proveer las transiciones de la señal para que los relojes puedan ajustarse en el extremo receptor, para mantener la sincronización.

Antes de describir las características de estos protocolos de enlace de datos, es útil una breve referencia hacia la terminología popularmente usada. La tabla 2.6 lista los términos. Tres atributos claves ayudan para diferenciar entre estos protocolos de enlace de datos seriales síncronos (LAPB, HDLC, y PPP):

- Si el protocolo soporta comunicaciones síncronas, comunicaciones asíncronas, o ambos.
- Si el protocolo proporciona la recuperación de error. (Los protocolos LAPB, HDLC, y PPP proporcionan detección de error.)
- Si existe un campo tipo protocolo. En otros términos, las especificaciones del protocolo definen un campo en la cabecera que identifica el tipo de paquete contenido en la porción de los datos de la trama.

Tabla 2.6 Terminología WAN

Termino	**Definición**
Síncrono	La imposición del ordenamiento de tiempo en un caudal de bits. Hablando más prácticamente, un dispositivo intentará usar la misma velocidad como el otro en el otro extremo de un enlace serie. Sin embargo, examinando las transiciones entre los estados de voltaje en el enlace, el dispositivo puede notar variaciones ligeras en la velocidad en cada extremo para que pueda ajustar su velocidad.
Fuente de reloj	El dispositivo el cual los otros dispositivos en el enlace ajustan su velocidad al usar enlaces síncronos.
asíncrono	La falta de un ordenamiento de tiempo impuesto en un caudal de bits. Particularmente hablando, ambos lados acuerdan la misma velocidad, pero no hay ningún chequeo o ajuste de las velocidades si ellos son ligeramente diferentes. Sin embargo, ya que solo se envía 1 byte por el traslado, las diferencias ligeras en la velocidad de reloj no son un problema. Un bit de salida se usa para señalar el principio de un byte.
DSU/CSU	Es la Unidad de Servicio de Datos y la Unidad de Servicios de Canal. Esto se usa en los enlaces digitales como una interfase para la compañía de teléfonos en los Estados Unidos. Los ruteadores usan un cable corto de una interfase serial hacia un DSU/CSU que se conecta a la línea de la compañía de teléfonos con una configuración similar al otro ruteador en el otro extremo del enlace. Los ruteadores usan su DSU/CSU conectada como la fuente de reloj.
Telco	Compañía de teléfonos
Circuito de 4 alambres	Una línea de la compañía telefónica con cuatro alambres, comprendida por dos pares trenzados de alambres. Cada par se usa para enviar en una dirección, así que un circuito de 4 alambres permite la comunicación full duplex.
Circuito de 2 alambres	Una línea de una compañía telefónica con dos alambres, comprendida de un alambre de par trenzado. El par se usa para enviar en solo una dirección a la vez, así que un circuito de 2 alambres permite sólo comunicación half duplex.
T/1	Es una línea de compañía telefónica que permite transmisión de datos a las 1.544 Mbps. Esto puede usarse con un multiplexor T/1.
T/1 MUX	Es un multiplexor que separa el T/1 en 24 canales diferentes de 64 Kbps. En los Estados Unidos, uno de cada 8 bits en cada canal puede ser usado por el compañía telefónica para que los canales sean canales de 56 Kbps efectivos.
E/1	Como un T/1, pero en Europa. Usa una velocidad de canales de 2.048 Mbps y 32 64 Kbps cauces.

Primero, unas palabras sobre el criterio usado para comparar estos protocolos WAN podrían demostrar ser útiles. Los protocolos síncronos permiten una mayor transferencia de datos sobre un enlace serial que los protocolos asíncronos. Sin embargo, los protocolos asíncronos requieren hardware menos caro, debido a que no hay necesidad para mirar las transiciones y ajustar la velocidad del reloj. Para los enlaces entre los ruteadores, típicamente se requieren enlaces síncronos. Todos los protocolos cubiertos en esta sección soportan enlaces síncronos.

Otro criterio de comparación es la recuperación de error. Todos los protocolos descritos aquí usan un campo en el remolque, normalmente llamado la secuencia de chequeo de trama (FCS), que se usa para verificar si ocurrieron errores de bits durante la transmisión de la trama. Si eso sucede, la trama se desecha. La recuperación de error es el proceso que causa la retransmisión de tramas perdidas; la recuperación de error puede realizarse por el protocolo de enlace de datos o por un protocolo de capa superior, de lo contrario, la recuperación de error no podría realizarse del todo. Los datos indiferentes, todos los protocolos de enlace de datos realizan la detección de error, el cual involucra la notificación del error y el desecho de la trama.

Finalmente, la definición y el uso de un campo tipo arquitectura de Protocolo es el último criterio para la comparación. Cada protocolo de enlace de datos que soporta múltiples protocolos de la capa de red, necesita un método de definición del tipo de paquete encapsulado dentro de la trama WAN de enlace de datos. Si tal campo es parte de la especificación del protocolo, es considerado "arquitectado", en otras palabras, especificadas en el protocolo. La tabla 2.7 lista estos protocolos de enlace de datos punto a punto y sus atributos.

Tabla 2.7 Atributos del protocolo de enlace de datos punto a punto

Protocolo	¿Corrección de error?	¿Campo de tipo de arquitectura?	Otros atributos
Synchronous Data Link Control (SDLC)	Si	Nulo	SDLC soporta enlaces multipunto; asume que la cabecera SNA ocurre después de la cabecera SDLC.
Link Access Procedure Balanced (LAPB)	Si	Nulo	La especificación asume un solo protocolo configurable después de LAPB. LAPB se usa principalmente con X.25. Cisco usa un campo de tipo de propietario para soportar el tráfico del multiprotocolo.
Link Access Procedure on the D channel (LAPD)	No	No	LAPD no se usa entre los ruteadores, pero es usado en el canal D desde el ruteador hacia el switch ISDN para la señalización
High-Level Data Link Control (HDLC)	No	No	HDLC sirve como el valor predefinido de Cisco en los enlaces seriales. Cisco usa un campo de tipo de propietario para soportar el tráfico del multiprotocolo.
Protocolo punto a punto (PPP)	Le permite al usuario que escoja si la corrección de error se ha realizado; la corrección usa LAPB	Si	PPP se hizo para la interoperabilidad del multiprotocolo de su principio, al contrario de todos los otros. PPP también soporta la comunicación asíncrona.

2.8.1. Compresión

La compresión puede realizarse en enlaces punto a punto LAPB, HDLC, y PPP. La meta de la compresión es reducir el número de bytes enviados por el enlace. Sin embargo, Hay un precio que pagar para la compresión, ciclos de CPU y el posible incremento de la latencia para los paquetes. La lista siguiente resume el dilema al considerar si se debe usar la compresión:

- Más procesamiento se requiere en el ruteador para comprimir cada trama, a comparación de cuando no hay compresión.
- La latencia por trama se incrementara debido al proceso requerido.
- La latencia por trama disminuirá en los casos cuando los paquetes sin comprimir han esperado en la cola del resultado debido a la congestión del enlace. Con las tramas comprimidas, la cola es más corta.
- La utilización del enlace disminuirá.

Así que, en casos en que las líneas arrendadas son caras o una línea más rápida no puede justificarse, entonces la compresión puede ser deseable. Sin embargo, debe tenerse cuidado para evitar la utilización excesiva del CPU. Cisco recomienda evitar mantener la utilización del CPU que exceda entre el 40 y 65 por ciento, dependiendo de la plataforma.

2.9. Protocolos Frame Relay

Frame Relay proporciona la entrega de tramas de datos variantes en tamaño para múltiples sitios Wan conectados. A diferencia de los enlaces punto a punto, Frame Relay es el protocolo más típicamente visto

Frame Relay es un nombre bien escogido para recordarle que se relaciona más estrechamente a la capa 2 de OSI. El término Frame es generalmente asociado con una colección de bits datos que incluyen una cabecera equivalente de capa 2 de OSI. Por ejemplo, una trama Ethernet incluye la cabecera/remolque Ethernet. Frame Relay usa direcciones, pero ese direccionamiento no intenta crear una estructura de dirección lógica que podría usarse sobre una variedad de medios de comunicación; por consiguiente, el direccionamiento Frame Relay es más cercano a los estándares de direccionamiento de la capa 2 de OSI y se considera a ser un protocolo de capa 2.

2.9.1. Características de Frame Relay y terminología

Frame Relay es una red multiacceso, la cual, realmente significa que más de dos dispositivos pueden conectarse al medio. El multiacceso es el primer y más obvia diferencia entre Frame Relay y las líneas arrendadas. Sin embargo, se usan las líneas arrendadas como el componente del enlace de acceso a redes Frame Relay. Considere la figura 2.2 la cual es un recurso valioso para repasar los conceptos de Frame Relay.

El enlace de acceso entre el ruteador y el switch Frame Relay, es una línea arrendada. Se conectan ambos sitios representados en la figura 2.2 hacia algún switch cercano por medio de una línea arrendada. El proveedor de servicio interconecta sus switches para proporcionar la conectividad La tabla 2.7 listas los componentes en la Figura 8-4 y algunos términos relacionados.

Figura 2.2 Componentes de Frame Relay

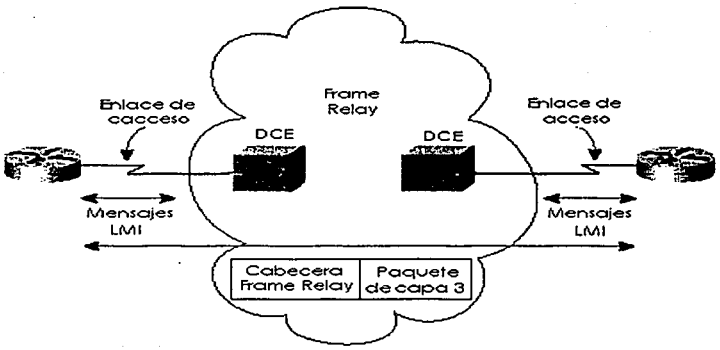


Tabla 2.7 Conceptos y términos de Frame Relay

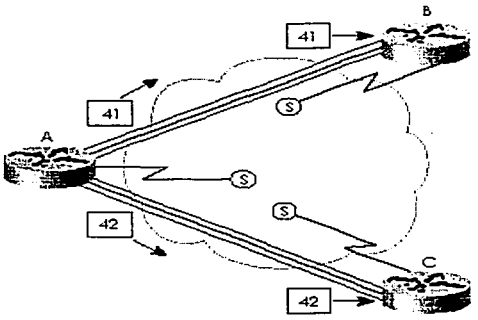
Circuito Virtual (VC)	Un VC es un concepto lógico que representa el camino que las tramas viajan entre DTEs. VCs son particularmente útiles al comparar Frame Relay con los circuitos físicos arrendados
Circuito Virtual Permanente	Un PVC es un VC que esta predefinido. Un PVC puede igualarse a una línea arrendada en concepto.
Circuito Virtual Swithceado	Un SVC es un VC que esta configurado dinámicamente. Un SVC puede igualarse a una conexión de dial en concepto.
Equipo Terminal de Datos (DTE)	Los DTEs también son conocidos como equipo de terminación de circuito de datos. Por ejemplo, los ruteadores son DTEs cuando están conectados a un servicio Frame Relay de una compañía de telecomunicaciones.
Enlace de Acceso	El enlace de acceso es la línea arrendada entre un DTE y un DCE.
Proporción de información comprometida (CIR)	El CIR es la tasa a la cual el DTE puede enviar los datos para un VC individual, con el cual el proveedor se compromete a entregar esa cantidad de datos. El proveedor enviará cualquier exceso de datos de esta tasa para este VC, si su red tiene la capacidad en ese momento. Esta opción afecta típicamente el precio de cada CV.
Tasa de ráfaga	La tasa de ráfaga es la tasa de longitud y tiempo, para el cual, en un VC en particular, el DTE puede enviar más rápidamente que el CIR, y el proveedor está de acuerdo en remitir los datos. Esta opción típicamente afecta el precio de cada VC.
Identificador de conexión de enlace de datos (DLCI)	Un DLCI es una dirección Frame Relay se usa en las cabeceras Frame Relay para identificar el circuito virtual.
Notificación de congestión explícita adelantada (FECN)	El FECN es el bit en la cabecera Frame Relay que señala a cualquiera recibiendo la trama (switches y DTEs) que la congestión está ocurriendo en la misma dirección de la trama. Los switches y DTEs pueden reaccionar retardando la tasa a la cual los datos se envían en esa dirección.

Notificación de congestión explícita retrasada (BECN)	El BECN es el bit en la trama Frame Relay que señala a cualquiera recibiendo la trama (Iswitches y DTEs) que la congestión está ocurriendo en la dirección opuesta (hacia atrás) de la trama. Los switches y DTEs pueden reaccionar retardando la tasa por la cual los datos se envían en esa dirección.
Desechar elegibilidad (DE)	El DE es el bit en la cabecera Frame Relay que señala hacia un switch para saber, si las tramas deben ser desechadas, por favor escoja esta trama para desechar en lugar de otra trama sin el bit DE puesto.
Multiacceso de monobroadcast (NBMA)	NBMA se refiere a una red en la cual las transmisiones no son soportadas, pero más dedos dispositivos pueden conectarse.
Interfase de Dirección local (LMI)	LMI es el protocolo usado entre un DCE y DTE para manejar la conexión. Los mensajes de la señalización para SVCs, mensajes de estado PVC, y keepalives son todos mensajes LMI.
Procedimiento de acceso al enlace, servicio portador modo trama (LAPF)	LAPF es la cabecera y trailer básica de Frame Relay; incluye DLCI, FECN, BECN, y bits DE.

2.9.2. Direccionamiento DLCI y switchweo Frame Relay

El identificador de la conexión de enlace de datos (DLCI) es la dirección Frame Relay. Los DLCI, no los DTE, son usados para direccional circuitos virtuales. Esta diferencia es principalmente debida al uso del DLCI y el hecho de que hay un solo campo DLCI en la cabecera, no es una fuente y destino DLCI. Los DLCI's son usados para direcciones el circuito virtual (VC). Por ejemplo, en la figura 2.3, el ruteador A tiene un VC en ambos ruteadores B y C; el ruteador A necesitara usar un DLCI diferente para cada VC. Los switches Frame Relay cambian el transito DLCI. Por ejemplo, el ruteador A envía una trama con un DLCI 41, esperando que sea entregada al ruteador B. Así como, el ruteador A envía las tramas con un DLCI 42 cuando quiere entregar la trama al ruteador C.

Figura 2.3 Direccionamiento Frame Relay

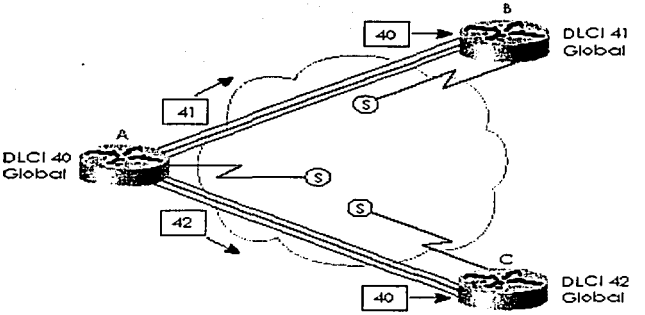


Los DLCI de Frame Relay son localmente significantes; esto significa que las direcciones necesitan ser únicas solo en el enlace de acceso local. Una analogía popular que explica el direccionamiento local es que puede haber una sola dirección de calle de Avenida Pennsylvania 2000, Washington,

D.C., pero puede haber una Avenida de Pennsylvania 2000 en cada ciudad en los Estados Unidos. Así como, DLCIs deben ser únicos en cada enlace de acceso.
Los DLCI deben ser únicos en cada enlace de acceso. El DLCI usado para identificar un VC individual en un enlace de acceso, no tiene que llevar el valor que se escoge para identificar el VC en el enlace de acceso, al otro extremo del VC.

Con la convención mostrada en la figura 2.4, los valores del DLCI son diferentes en cada extremo del VC. Sin embargo, los valores mostrados en la figura 2.3, también son válidos. En la práctica, el estilo mostrado en la figura 2.4, es la típica opción, pero parece ser un poco más confusa. ¿Pero por que? La respuesta queda en un término llamado direccionamiento global.

Figura 2.5 Direccionamiento local Frame Relay, con DLCI diferentes en cada extremo



El concepto de direccionamiento global es la razón por la cual las redes Frame Relay típicas usan un valor de DLCI diferente en cada extremo del VC. El direccionamiento global le permite pensar en la red Frame Relay como una LAN en lo que se refiere a conceptos de direccionamiento. Considere la figura 2.5 con los valores del DLCI mostrados. En esta figura, piense en los valores del DLCI como una dirección para el DTE la cual es similar a como una dirección MAC unicast representa una tarjeta LAN.

En una LAN, si el host B quiere enviar a una trama al host A, El host B envía una trama con la dirección MAC del host A como el destino. Similarmente, si el ruteador B quiere enviar una trama hacia el ruteador A, entonces el ruteador B (por la convención del direccionamiento global) envía una trama con el valor DLCI global en la cabecera del ruteador A. Así como, el ruteador C envía las tramas con un DLCI 40 para alcanzar al ruteador A por la convención. El ruteador A envía las tramas con DLCI 41 para alcanzar al ruteador B, y con un DLCI 42 para alcanzar al ruteador C, de nuevo, por la convención de direccionamiento global. La figura 2.6 muestra que los DLCIs usados para el direccionamiento global y los valores reales puestos en las cabeceras Frame Relay para la entrega correcta por la red. La tabla 8-12 resume los DLCIs usados en la figura.

Figura 2.6 Convención del direccionamiento global de Frame Relay, con la realidad del direccionamiento local

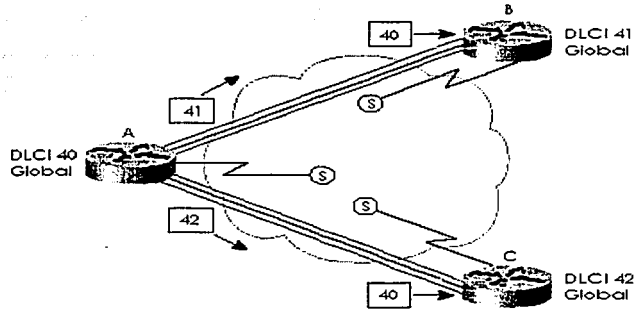


Tabla 2.8 Intercambio DLCI en la Nube Frame Relay

Trama enviada por el ruteador . . .	Con el campo DLCI	Se entrega en el ruteador . . .	Con el campo DLCI
A	41	B	40
A	42	C	40
B	40	A	41
C	40	A	42

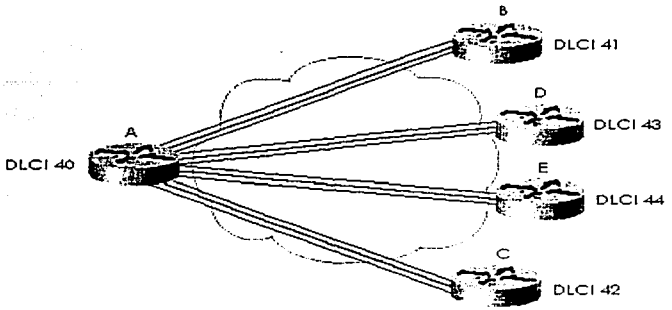
La figura 2.6 muestra una trama siendo enviada del ruteador A hacia el ruteador B en un caso, y hacia el ruteador C en el otro caso. Como el ruteador A envía una trama con un DLCI 41, los switches Frame Relay envían la trama hacia el ruteador B. Antes de ser enviadas en el enlace de acceso hacia el ruteador B, el switch final cambia el DLCI a 40 para que el ruteador B sepa quién envió la trama. Similarmente, el ruteador A envía una trama con DLCI 42, y se recibe por el ruteador C con DLCI 40.

De hecho, los DLCIs usados coinciden con la red de muestra con direccionamiento local de la figura 2.5. En esencia:

- El direccionamiento local es como trabaja el direccionamiento Frame Relay. Sin embargo, siguiendo la convención del direccionamiento global, planear es más fácil porque el direccionamiento parece similar al direccionamiento LAN.
- Una dirección global para un DTE simplemente significa que todos los otros DTEs con un VC hacia este DTE usa esta dirección global en su enlace de acceso global

Un beneficio particularmente conveniente del direccionamiento local es que nuevos sitios pueden agregarse con más conveniencia. Examine la figura 2.7, con los ruteadores D y E agregados. El proveedor de servicio simplemente establece que los DLCI global 43 y 44 serán usados para estos dos ruteadores. Si estos dos ruteadores también tienen solo un PVC hacia el ruteador A, todo el planeo DLCI esta completo. Se sabe que el ruteador D y el ruteador E usara el DLCI 40 para alcanzar el ruteador A, y que el ruteador A usara el DLCI 43 para alcanzar el ruteador D y un DLCI 44 para alcanzar el ruteador E.

Figura 2.7 Adición de sitios Frame Relay: Direccionamiento global



Las muestras restantes en este capítulo usan el direccionamiento global en cualquier diagrama de planeación, a menos que por otra parte se establezca. Una manera práctica de determinar si el diagrama liste los DLCIs locales, o la convención DLCI global es esta: Si dos VCs terminan en un DTE y se muestra solo un DLCI, entonces probablemente represente la convención global DLCI. Si se muestra un DLCI por VC, entonces está pintando el direccionamiento local DLCI.

2.9.3. La capa de la red tiene relación con Frame Relay

Los especialistas en redes, deberán tener en cuenta tres problemas claves con la capa 3 corriendo sobre Frame Relay:

- Las opciones para las direcciones de la capa 3 en las interfaces Frame Relay
- Manejo de Transmisión
- Horizonte partido

2.10. ISDN

2.10.1. Uso típico

ISDN se usa típicamente para las conexiones de marcación de discado temporal. El costo atractivo también ha causado que algunas compañías usen permanentemente conexiones ISDN, en lugar de las líneas arrendadas. Las líneas ISDN pueden proporcionar el acceso a 128 Kbps, usando ambos canales B. La compresión puede aumentar el rendimiento, obteniendo potencialmente 500 Kbps de rendimiento a través de la línea.

Las conexiones temporales entre los ruteadores, es otro uso típico de ISDN, ambos para el respaldo y para la conexión ocasional. Las conexiones ocasionales incluirían el tráfico para los sitios que no usan aplicaciones en línea o vídeo conferencia, y casos en los cuales se desea un ancho de banda adicional entre los sitios. La mayoría de las configuraciones necesarias para estas conexiones ocasionales se relaciona a un tema llamado ruteo de marcación bajo demanda (Dial-On-Demand Routing - DDR)

Los escenarios en la figura 2.8 pueden describirse de la manera siguiente:

Caso 1 muestra el ruteo de marcación bajo demanda. La lógica se configura en los ruteadores para disparar la marcación de discado cuando el tráfico que necesita llegar a otro sitio es enviado por el usuario.

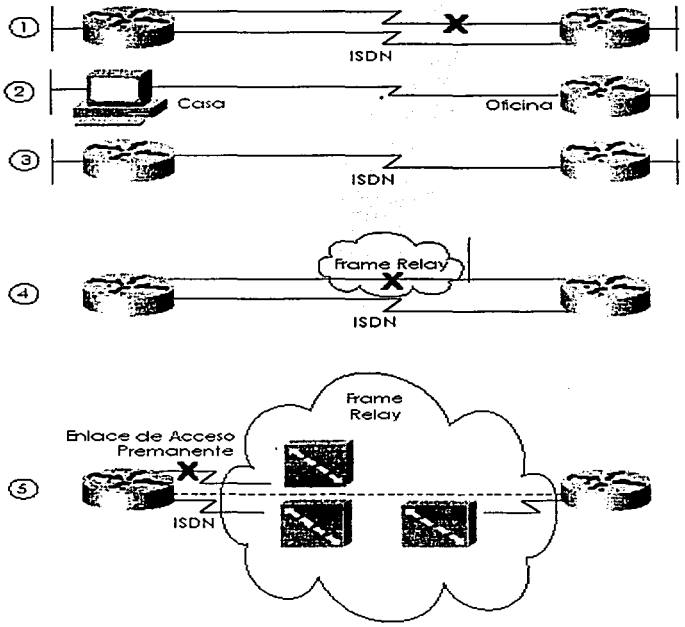
Caso 2 muestra un ambiente del telecommuting típico.

Caso 3 muestra la típica topología de marcación de discado de respaldo. La línea arrendada falla, así que una llamada ISDN se establece entre los mismos dos ruteadores.

Caso 4 muestra un caso en que un ISDN BRI podría ser usado para marcar directamente hacia otro ruteador para reemplazar un enlace de acceso Frame Relay o un VC fallido.

Caso 5 describe una línea ISDN que podría usarse para marcar en la red Frame Relay del proveedor, reemplazando un VC fallido o enlace de acceso con un VC corriendo sobre una conexión ISDN hacia el switch Frame Relay.

Figura 2.8 Conexiones Ocasionales Típicas Entre los Ruteadores



2.11.2. Multienlace PPP

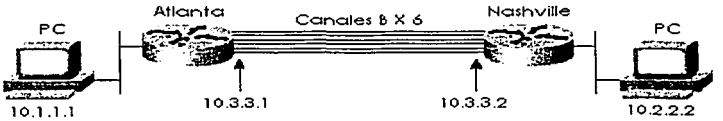
El multienlace PPP es una función que permite enlaces múltiples entre un ruteador y algún otro dispositivo sobre el cual, el tráfico es balanceado. De cuándo usarlo es sutil. La figura 2.9 ilustra la necesidad más obvia para el Multienlace PPP.

Figura 2.9 Multienlace PPP para en el dispositivo

Para un servicio más rápido, la PC que ha marcado querría usar ambos canales B eficazmente. La figura 2.9 muestra dos lineas punteadas entre la PC y el servidor de acceso, significando que dos canales B están en uso entre los dispositivos. El multienlace PPP rompe un paquete en fragmentos, envía algunos fragmentos a través de cada uno de los dos enlaces, y los vuelve a ensamblar en el otro extremo del enlace. La red resultante es que los enlaces se utilizan aproximadamente a la misma cantidad.

El multienlace PPP también es útil entre los ruteadores. Por ejemplo, en la figura 2.10, teniendo una videoconferencia entre Atlanta y Nashville se usan seis canales B entre dos ruteadores.

Figura 2.10 Canales B Múltiples Entre los Ruteadores



En este ejemplo, si se usa multienlace PPP, los enlaces tienen la utilización casi idéntica. Lo negativo es que los ruteadores deben fragmentar y deben volver a ensamblar cada paquete. Sin embargo, los 384 Kbps necesarios para la video conferencia están disponibles.

Ahora considere la alternativa, sin el multienlace PPP, pero simplemente con PPP en cada uno de los seis enlaces. Seis rutas hacia la subred 10.2.2.0/24 existirían en la tabla de ruteo del Ruteador A. Con cualquiera de los métodos más rápidos de switcheo internos en un ruteador de Cisco (El switcheo rápido, el switcheo óptimo, switcheo NetFlow), el efecto de balanceo es que todos los paquetes hacia la misma dirección IP usan el mismo enlace. El resultado es que el ruteador Atlanta envía algunos paquetes sobre un enlace y algunos sobre el otro, pero el equilibrio es imprevisible. Más importantemente, todos los paquetes hacia la dirección IP única del sistema de videoconferencia en Nashville usará el mismo enlace, limitando la videoconferencia hasta 64 Kbps eficaces. Una alternativa es desactivar los métodos más rápidos de switcheo en el ruteador para que se usen múltiples rutas hacia la misma subred. Sin embargo, eso no se recomienda debido a que retarda el procesamiento interior significativamente en el ruteador. Por esa razón, el multienlace PPP es una opción buena en este caso.

El ejemplo 2.1 muestra una configuración de un multienlace PPP. Los ruteadores Atlanta y Nashville usarán dos canales B del mismo BRI.

Ejemplo 2.1 Configuración Multienlace PPP para Atlanta

```
username Nashville password Robert
interface bri 0
ip addr 10.3.3.1 255.255.255.0
encapsulation ppp
dialer idle-timeout 300
dialer load-threshold 25 either
dialer map 10.3.3.2 name Nashville 16155551234
dialer-group 1
ppp authentication chap
ppp multilink
```

Los dos comandos importantes son el **ppp multilink** y los comandos **dialer load-threshold.** El ppp multilink habilita el multienlace PPP; dialer load-threshold le dice al ruteador que marque a otro canal B si el promedio de utilización en los enlaces actualmente usados es más de 25 por ciento para cualquier utilización entrante o saliente

2.11.3. Ruteo bajo demanda y configuración ISDN

DDR define la lógica detrás de cuando un ruteador escoge marcar otro sitio, si se usa ISDN, serial síncrona, o si se usan interfaces seriales asíncronas.; la lógica de DDR es la misma para cualquiera de los tres tipos de interfaces de marcación.

Tabla 2.10 Comandos EXEC ISDN relacionados

Comando	Función
show interfaces bri number[:b-channel]	Incluye la referencia hacia las listas de acceso habilitadas en la interfase.
show controllers bri number	Muestra las estadísticas y el estado de la capa 1 para los canales B y D.
show isdn {active | history | memory | status | timers}	Muestra información variada de estado ISDN.
show interfaces bri number[[:bchannel] | [first] [last]] [accounting]	Despliega la información de la interfase acerca del canal D o los canales B.
show dialer interface bri number	Las listas los parámetros DDR en la interfase BRI. Muestra si actualmente se ha marcado, indicando el estado actual. También muestra intentos previos para marcar y si tuvieron éxito.
debug isdn q921	Listas los mensajes ISDN de la capa 2.
debug isdn q931	Lista los mensajes ISDN de la capa 3 (llamados setup/teardown).
debug dialer {events | packets}	Lista la información cuando un paquete se dirige fuera de una interfase de marcación, diciendo si el paquete es interesante.

Tabla 2.9 Comandos de Configuración ISDN

Comando	Modo de configuración	Propósito
isdn switch-type switch-type	Global o Interfase	Define al ruteador el tipo de switch ISDN el cual la línea ISDN se conecta en la oficina central.
isdn spid1 spid.	Interfase	Define el primer SPID
isdn spid2 spid.	Interfase	Define el segundo SPID
isdn caller number	Interfase	Define un número válido para las llamadas entrantes al usar la proyección de llamada.
isdn answer1 [called-party-number][:subaddress]	Interfase	Especifica el número ISDN o subdirección que debe usarse en las llamadas entrantes para que este ruteador conteste.
isdn answer2 [called-party-number][:subaddress]	Interfase	Especifica un segundo número ISDN o subdirección que debe usarse en las llamadas entrantes para que este ruteador conteste.
dialer-list [list nnn] protocol[protocol-type] permit | deny	Global	Define el tipo de tráfico considerado interesante.
dialer-group n	Interfase	Habilita la lista de marcaje en esta interfase.
dialer in-band	Interfase	Habilita la marcación dentro y la marcación dentro en esta interfase. Este comando sólo se usa para líneas seriales que se conectan hacia un TA, no para interfaces ISDN nativas que usan el canal D fuera de banda.
dialer string string	Interfase	Es el cordón del marcación usado al marcar un sólo sitio.
dialer map protocol next-hop address [name hostname] [speed 56 | 64][broadcast] dial-string	Interfase	Es el cordón de marcación para alcanzar el siguiente salto. Sin embargo, el comando map se usa al marcar más de un sitio. Este también es el nombre usado para la autenticación. La transmisión se asegura que las copias de transmisiones vayan hacia esta dirección del siguiente salto.

Capitulo 3 Configuraciones y Simuladores

3.1. Introducción

En este capítulo se muestran varias configuraciones con una breve explicación de los casos más comunes en los que nos involucraremos en el desarrollo de las prácticas, además se mostrará una el funcionamiento de una herramienta indispensable para el desarrollo de las configuraciones.

3.2. Configuración básica del switch 1900

En el switch Catalyst 1900, existen tres métodos de configuración diferentes:

- Menú de la interfase manejada del puerto de la consola
- Manejo de switch visual basado en la Web (VSM)
- IOS línea de comandos de la interfase (CLI)

Tabla 3.1 Comandos de configuración para el switch Catalyst 1900

Comando	Descripción
ip address dirección máscara – subnet	Establece la dirección IP del switch
ip default-gateway	Establece la pasarela de entrada predefinida para que la interfase de manejo pueda alcanzarse de una red remota
show ip	Despliega la configuración de las direcciones IP
show interfaces	Despliega la información de la interfase
mac-address-table permanent tipo de dirección MAC módulo /puerto	Establece una dirección MAC permanente
port secure [max-mac-count conteo]	Establece una dirección MAC estática restringida
show mac-address-table (seguridad)	Establece la seguridad del puerto
address-violation {suspend | disable | ignore}	Despliega la tabla de direcciones MAC; la opción de seguridad despliega la información sobre el establecimiento restringido o estático
show versión	Despliega la información de la versión
copy tftp://10.1.1.1/config.cfg nvram	Copia un archivo de configuración del servidor TFTP a la dirección IP 10.1.1.1.
copy nvram tftp://10.1.1.1/config.cfg	Salva un archivo de configuración al servidor TFTP a la dirección IP 10.1.1.1.
delete nvram	Quita todos los parámetros de configuración y pone en el switch las especificaciones predefinidas de fábrica

3.2.1. Configuración predefinida del switch 1900

Los valores predefinidos varían dependiendo de las características del switch. La lista siguiente provee algunas de las especificaciones predefinidas para el switch Catalyst 1900. (No todos los valores predefinidos se muestran en este ejemplo.)

- **Dirección IP**: 0.0.0.0
- **CDP**: Enabled
- **Modo de switcheo**: FragmentFree
- **Puerto: 100BaseT**: Auto-negociate duplex mode
- **Puerto: 10BaseT**: Half dúplex
- **Arbol de expansión**: Enabled
- **Contraseña de consola**: None

Similar al sistema operativo del ruteador, el switch Catalyst 1900 tiene varios modos de configuración. El ejemplo 3.1 muestra la configuración inicial IP y dúplex, con el indicador (Prompt) actual mostrando los muy familiares modos EXEC y configuración.

Ejemplo 3.1 Modos de configuración para configurar IP y duplex

```
wg_sw_a# configure terminal
wg_sw_a(config)#ip address 10.5.5.11 255.255.255.0
wg_sw_a(config)#ip default-gateway 10.5.5.3
wg_sw_a(config)# interface e0:1
wg_sw_a(config-if)#duplex  half
wg_sw_a(config-if)#end
wg_sw_a
```

En el ejemplo, el dúplex podría establecerse a uno de los modos siguientes:

- **Auto** - Establece la auto negociación del modo duplex. Esta es la opción predefinida para los puertos TX de 100 Mbps
- **full** - establece el modo full duplex
- **full-flow-control** - Establece el modo con control de flujo.
- **half** - establece el modo half-duplex. Ésta es la opción predefinida para puertos TX de 10 Mbps.

Para verificar la configuración IP y el establecimiento del dúplex en una interfase dada, use los comandos **show ip** y **show interfase**, como se ve en el ejemplo 3.2. Nótese que no hay ninguna dirección IP en el resultado de **show interfase**, porque la dirección IP es asociada con todo el switch, no sólo a una interfase. Se muestra el estado del Árbol de expansión de la interfase, como en la configuración del duplex. Si el dúplex se desigualara con el dispositivo en el otro extremo, el contador de colisiones probablemente se incrementaría rápidamente mas tarde.

Ejemplo 3.2 Resultado de show ip y show interfaces

```
wg_sw_a#show ip
IP address: 10.5.5.11
Subnet mask: 255.255.255.0
Default gateway: 10.5.5.3
Management VLAN:  1
Domain name:
Name server 1: 0.0.0.0
Name server 2: 0.0.0.0
HTTP server: Enabled
HTTP port:  80
RIP: Enabled
wg_sw_a#
wg_sw_a#sh interfaces

Ethernet 0/1 is Enabled
Hardware is Built-in 10Base-T
Address is 0090.8673.3341
MTU 1500 bytes, BW 10000 Kbits
802.1d STP State:  Forwarding     Forward Transitions:  1
Port monitoring: Disabled
Unknown unicast flooding: Enabled
Unregistered multicast flooding:  Enabled
```

```
Description:
Duplex setting: Half duplex
Back pressure: Disabled

    Receive Statistics                         Transmit Statistics
--------------------------------------     -------------------------------------
Total good frames                 44841    Total frames                   404502
Total octets                    4944550    Total octets                 29591574
Broadcast/multicast frames        31011    Broadcast/multicast frames     390913
Broadcast/multicast octets      3865029    Broadcast/multicast octets   28478154
Good frames forwarded             44832    Deferrals                           0
Frames filtered                       9    Single collisions                   0
Runt frames                           0    Multiple collisions                 0
No buffer discards                    0    Excessive collisions                0
                                           Queue full discards                 0
Errors:                                    Errors:
  FCS errors                          0      Late collisions                   0
  Alignment errors                    0      Excessive deferrals               0
  Giant frames                        0      Jabber errors                     0
  Address violations                  0      Other transmit errors             0
```

3.3. Configuración básica de VLAN

En esta sección se discuten las pautas a seguir para configurar VLANs en el switch Cisco 1900. Deben recordarse varias cosas antes de empezar con la configuración VLAN:

- El número máximo de VLANs depende del switch. El Catalyst 1900 soporta 64 VLANs con un árbol de expansión separado por VLAN.
- VLAN1 es un valor predeterminado de fábrica VLANs.
- Se envían anuncios CDP y VTP en la VLAN1.
- La dirección IP del Catalyst 1900 está en el dominio de transmisión de la VLAN1.
- El switch debe estar en el modo de servidor VTP para crear, agregar, o borrar VLANs.

Un término no cubierto todavía en esta lista es el Protocolo Troncal VLAN (VLAN Trunking Protocol - VTP). VTP es un protocolo de mensajería de la capa 2 que mantiene la consistencia de la configuración a lo largo de un dominio de administración común. VTP logra esta meta manejando las adiciones, el borrado, y los cambios de nombre de las VLANs a través de las redes. VTP minimiza las configuraciones erróneas e inconsistencias de configuración que puedan causar problemas, tales como nombres de VLAN dobles o tipo de especificaciones VLAN incorrectas.

Para configurar las características de VLAN, los switches necesitarán ser configurados en modo transparente VTP.

Tabla 3.2 Lista de comandos VLAN

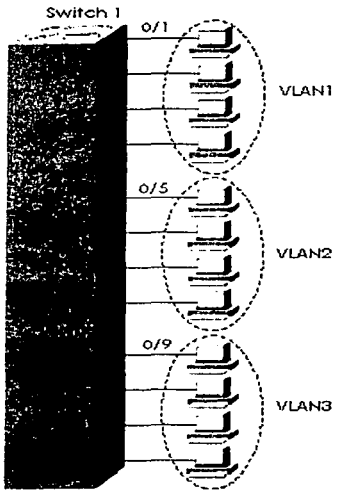
Comando	Descripción
delete vtp	Restablece todos los parámetros VTP a los valores predefinidos y restablece el número de revisión de configuración a 1
vtp [server | transparent | client] [domain dominio-nombre] **[trap {enable | disable}] [password** contraseña] **[pruning {enable | disable}]**	Define los parámetros VTP
vtp trunk pruning-disable lista- vlan	Desactiva el recorte para VLANs específicas en una interfase troncal en particular (subcomando de la interfase)
show vtp	Despliega el estado del VTP
trunk [on | off | desirable | auto | nonegotiate]	Configura una interfase de la troncal
show trunk	Despliega el estado de la troncal
vlan vlan **# name** nombre de la vlan	Define una VLAN y su nombre
show vlan	Despliega la información de la VLAN
vlan-membership static vlan#	Asigna un puerto a una VLAN
show vlan-membership	Despliega el número de miembros de la VLAN
show spantree vlan#	Despliega la información del árbol de expansión para una VLAN

3.3.1. Configuración de muestra para un Solo switch

Cuando el VTP no está en uso (en otras palabras, cuando el VTP esta en uso en modo transparente), la configuración de la VLAN consiste en tres tareas primarias:

Primero, usar el comando de configuración global **vtp** para configurar el modo transparente del VTP. Use el comando global **vlan** para definir cada número VLAN (requerido) y el nombre asociado (opcional). Entonces asignar cada puerto a su VLAN asociado que usando el subcomando de la interfase **vlan-membership**. El ejemplo 3.3 muestra un ejemplo, basado en Figura 3.1

Figura 3.1 Red de muestra, un switch, tres VLANs



Ejemplo 3.3 Configuración de un solo switch VLAN, coincide con la figura 4-28

```
switch(config)# vtp transparent domain dummy
switch(config)# vlan 2 name VLAN2
switch(config)# vlan 3 name VLAN3
switch(config)# interface e 0/5
switch(config-if)# vlan-membership static 2
switch(config-if)# interface e 0/6
switch(config-if)# vlan-membership static 2
switch(config-if)# interface e 0/7
switch(config-if)# vlan-membership static 2
switch(config-if)# interface e 0/8
switch(config-if)# vlan-membership static 2
switch(config-if)# interface e 0/9
switch(config-if)# vlan-membership static 3
switch(config-if)# interface e 0/10
switch(config-if)# vlan-membership static 3
switch(config-if)# interface e 0/11
switch(config-if)# vlan-membership static 3
switch(config-if)# interface e 0/12
switch(config-if)# vlan-membership static 3
```

Nótese que algunas configuraciones parecen estar faltando. La VLAN 1, con el nombre VLAN1, no se configura porque ya está configurada automáticamente. De hecho, el nombre no puede cambiarse. También, se considera que cualquier puerto sin una configuración VLAN estática específica, se considera que está en VLAN1. También, la dirección IP del switch se considera que está en el dominio de transmisión de la VLAN1. Se configuran los puertos del 5 al 8 estáticamente para la VLAN2; similarmente, la VLAN3 comprende los puertos desde el 9 al 12. Además, el VTP todavía sin ser explicado, se pone en modo transparente, con un nombre de dominio sin significado de comodín, este parámetro no es importante (todavía); simplemente debe ponerse.

Después de que la VLAN se configura, deben confirmarse los parámetros de esa VLAN para asegurar la validez. Para verificar los parámetros de una VLAN, use el comando EXEC privilegiado **show vlan** vlan # para desplegar la información sobre una VLAN en particular. Use **show vlan** para mostrar todas las VLANs configuradas El ejemplo 3.4 muestra el desempeño del comando **show**, el cual muestra los puertos del switch asignados a la VLAN.

Ejemplo 3.4 Muestra el desempeño VLAN

```
Switch1#sh vlan 3

VLAN Name                Status     Ports
-------------------------------------------
3    VLAN3               Enabled    9-12
-------------------------------------------

VLAN Type           SAID   MTU   Parent RingNo BridgeNo Stp  Trans1 Trans2
-------------------------------------------------------------------------
3    Ethernet       100003 1500     0     1       1     Unkn     0      0
-------------------------------------------------------------------------
```

Otros parámetros de VLAN mostrados en Ejemplo 3.4 incluyen el tipo (el valor predefinido es Ethernet), SAID (usado para troncales FDDI), MTU (el valor predefinido es 1500 para Ethernet VLAN), Protocolo de árbol de expansión (los switches 1900 soportan sólo la norma Protocolar 802.1D del árbol de expansión), y otros parámetros usados para Token Ring o VLANs FDDI.

3.4. Configuración IP

La tabla 3.3 y 3.4, resumen muchos de los comandos más comunes usados para la configuración IP y su comprobación. A continuación se presentan dos configuraciones de red de muestra, con ambas configuraciones y el resultado del comando EXEC.

Tabla 3.3 Comandos de configuración IP

Comando	Modo de configuración
ip address dirección-ip mascara **[secundaria]**	Modo interfase
ip host nombre [numero de puerto tcp] dirección1 [dirección2...dirección8]	Global
ip route prefijo de mascara {próximo brinco del ruteador | desempeño de la interfase}	Global
ip name-server dirección del servidor1 [[dirección del servidor2]...dirección del servidor6]	Global
ip domain-lookup	Global
ip routing	Global
ip netmask-format {bitcount | decimal | hexadecimal}	Modo interfase
ip default-network red	Global
ip classless	Global
ip host name [numero de puerto tcp] dirección1 [dirección2...dirección8]	Global

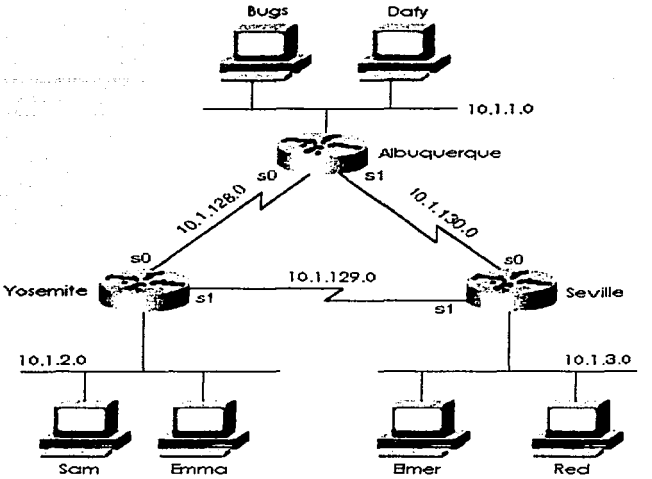
Tabla 3.4 Comandos IP EXEC

Comando	Función
show hosts	Lista todos los nombres de los host y las direcciones IP correspondientes
show interfaces [tipo numero]	Lista las estadísticas de la interfase, incluyendo la dirección IP
show ip interface [tipo numero]	Proporciona una vista detallada de los parámetros de configuración IP, por interfase
show ip interface brief	Proporciona un resumen de todas las interfaces y sus direcciones IP
show ip route [subred]	Muestra la tabla de ruteo, o una entrada si se introduce subred
show ip arp	Despliega la cache IP ARP
debug ip packet	Emite un registro del mensaje para cada paquete IP
terminal ip netmask-format {bitcount | decimal | hexadecimal}	Establece el tipo de desplegado para las mascaras de las subredes en los comandos show
Ping	Envía y recibe mensajes de eco ICMP para verificar la conectividad
Trace	Envía series de paquetes UDP con los valores TTL crecientes, para verificar la ruta actual hacia un host.

Colectivamente, la figura 3.2 y los ejemplos 3.5, 3.6, y 3.7 muestran tres sitios, cada uno con dos enlaces seriales y un enlace Ethernet. Las pautas siguientes del sitio fueron usadas al escoger los detalles de la configuración:

- Usar los nombres de los servidores a las direcciones 10.1.1.100 y 10.1.2.100.
- Usar los nombres del host de la figura *S-27*.
- Las direcciones IP del ruteador serán asignadas de las pocas últimas direcciones IP válidas en sus subredes conectadas; usar una máscara de 255.255.255.0.

Figura 3.2 Configuración de TCP/IP y Comprobaciones



Ejemplo 3.5 Configuración del ruteador de Albuquerque y comandos EXEC

```
Albuquerque#show running-config
Building configuration...

Current configuration:
!
version 11.2

hostname Albuquerque
!
enable secret 5 $1$skrNSz4oq60HfB6zu1%G4P/6ZY0
!
ip name-server 10.1.1.100
ip name-server 10.1.2.100
!
interface Serial0
 ip address 10.1.128.251 255.255.255.0
!
interface Serial1
 ip address 10.1.130.251 255.255.255.0
```

```
!
interface Ethernet0
 ip address 10.1.1.251 255.255.255.0
!
no ip classless
banner motd ^C
  Should've taken a left turn here! This is Albuquerque...  ^C
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end

Albuquerque#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

     10.0.0.0/24 is subnetted, 3 subnets
C       10.1.1.0 is directly connected, Ethernet0
C       10.1.130.0 is directly connected, Serial1
C       10.1.128.0 is directly connected, Serial0

Albuquerque#terminal ip netmask-format decimal
Albuquerque#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

     10.0.0.0 255.255.255.0 is subnetted, 3 subnets
C       10.1.1.0 is directly connected, Ethernet0
C       10.1.130.0 is directly connected, Serial1

C       10.1.128.0 is directly connected, Serial0
Albuquerque#
```

Ejemplo 3.6 Configuración del ruteador Yosemite y Comandos EXEC

```
Yosemite#show running-config
Building configuration...

Current configuration:
!
version 11.2

hostname Yosemite
!
enable secret 5 $1$.Iud$7uHq%zDYgvJN09v7HSkLZ/
!
ip name-server 10.1.1.100
ip name-server 10.1.2.100
!
interface Serial0
 ip address 10.1.128.252 255.255.255.0
 no fair-queue
!
interface Serial1
 ip address 10.1.129.252 255.255.255.0
!
interface Ethernet0
 ip address 10.1.2.252 255.255.255.0
!
no ip classless
banner motd ^C
   This is the Rootin-est Tootin-est Router in these here parts!  ^C
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end

Yosemite#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Serial0                10.1.128.252    YES manual up                    up
Serial1                10.1.129.252    YES manual up                    up
Ethernet0              10.1.2.252      YES manual up                    up
Yosemite#
```

Ejemplo 3.7 Configuración del ruteador Seville y comandos EXEC

```
Seville#show running-config
Building configuration...

Current configuration:
!
version 11.2

!
hostname Seville
!
enable secret 5 $1$ZvR/$Gpk5a5K5vTVpotd3KUygA1
!
ip name-server 10.1.1.100
ip name-server 10.1.2.100
!
interface Serial0
 ip address 10.1.130.253 255.255.255.0
 no fair-queue
!
interface Serial1
 ip address 10.1.129.253 255.255.255.0
!
Ethernet0
 ip address 10.1.3.253 255.255.255.0
!
no ip classless
banner motd ^C
  Take a little off the top, Wabbit!  (Elmer)   ^C
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end

Seville#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


10.0.0.0/24 is subnetted, 3 subnets
C       10.1.3.0 is directly connected, Ethernet0
```

```
C        10.1.130.0 is directly connected, Serial0
C        10.1.129.0 is directly connected, Serial1


Sevilla#show ip interface serial 1
Serial1 is up, line protocol is up
  Internet address is 10.1.129.253/24
  Broadcast address is 255.255.255.255
  Address determined by nonvolatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is enabled
  IP Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
 TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  Web Cache Redirect is disabled
  BGP Policy Mapping is disabled

Sevilla#show interface serial 0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.1.130.253/24
  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 00:00:05, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Queuing 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
     273 packets input, 18621 bytes, 0 no buffer
     Received 215 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     309 packets output, 20175 bytes, 0 underruns
     0 output errors, 0 collisions, 23 interface resets
```

```
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up

Seville#show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.3.102               0  0060.978b.1301  ARPA   Ethernet0
Internet  10.1.3.253               -  0000.0c3e.5183  ARPA   Ethernet0

Seville#debug ip packet
IP packet debugging is on
Seville#ping 10.1.130.251
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.130.251, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/81/84 ms
Seville#
00:09:38: IP: s=10.1.130.251 (local), d=10.1.130.251 (Serial1), len 100, sending
00:09:38: IP: s=10.1.130.251 (Serial1), d=10.1.130.253 (Serial1), len 100, rcvd 3
00:09:38: IP: s=10.1.130.253 (local), d=10.1.130.251 (Serial1), len 100, sending
00:09:38: IP: s=10.1.130.251 (Serial1), d=10.1.130.253 (Serial1), len 100, rcvd 3
00:09:38: IP: s=10.1.130.253 (local), d=10.1.130.251 (Serial1), len 100, sending
00:09:38: IP: s=10.1.130.251 (Serial1), d=10.1.130.253 (Serial1), len 100, rcvd 3
00:09:38: IP: s=10.1.130.253 (local), d=10.1.130.251 (Serial1), len 100, sending
00:09:38: IP: s=10.1.130.251 (Serial1), d=10.1.130.253 (Serial1), len 100, rcvd 3
00:09:38: IP: s=10.1.130.253 (local), d=10.1.130.251 (Serial1), len 100, sending
00:09:38: IP: s=10.1.130.251 (Serial1), d=10.1.130.253 (Serial1), len 100, rcvd 3
Seville#
```

Nótese que la configuración coincide con el resultado de los comandos **show interface**, **show ip interface**, y **show interface ip brief**. Por ejemplo, en el ejemplo 3.6, las direcciones IP en la configuración coinciden con el resultado del comando **show ip interface brief**. Si estos detalles no coinciden, es probable que este mirando la configuración en la NVRAM, y no en la RAM. Hay que asegúrese de usar los comandos **show running-config** o **write terminal** para ver la configuración activa.

La mascara de la subred en el resultado de los comandos show se codifican para numerar la red y los bits de la subred. Por ejemplo, 10.1.4.0/24 significan 24 bits de red y de subred, dejando 8 bits del host con este esquema de subnetting. El comando **terminal ip netmask** puede usarse para cambiar este formato, como se vio en el ejemplo 3.5.

El ejemplo 3.7 muestra la caché ARP, generada por el resultado del comando **show ip arp**. El primer ingreso muestra la dirección IP y la dirección MAC de otro host en el Ethernet. El valor 0 del cronómetro; implica que la entrada es muy reciente, el valor crece con el desuso. Se muestra una entrada para la interfase Ethernet mismo del ruteador el cual nunca se sale de tiempo de la tabla ARP.

El resultado del comando **debug ip packet** en el ejemplo 3.7, hace una lista de una ingreso por paquete IP enviado y recibido. Este comando es un comando muy peligroso, podría chocar casi cualquier producción del ruteador debido al agregado de cabeceras adicionales de procesamiento de los mensajes debug. Nótese que el resultado muestra las direcciones de fuente y destino.

La tabla de ruteo en el ejemplo 3.7, no lista todas las subredes porque la configuración del protocolo de ruteo, no se ha agregado. Nótese que los comandos **show ip route**, lista las rutas hacia la subred directamente conectada, pero no otras. Los comandos **ip route** en el ejemplo 3.8 han sido

agregados a Albuquerque. Los Ejemplos 3.9 y 3.10 contienen comandos show ejecutados después de que la nueva configuración fue agregada.

Ejemplo 3.8 Rutas Estáticas Agregadas a Albuquerque

```
ip route 10.1.2.0 255.255.255.0 10.1.128.252
ip route 10.1.3.0 255.255.255.0 10.1.130.253
```

Ejemplo 3.9 Comandos EXEC del ruteador Albuquerque, Después de que se agregaron las rutas estáticas para 10.1.2.0 y 10.1.3.0

```
Albuquerque#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

     10.0.0.0/24 is subnetted, 5 subnets
S       10.1.3.0 [1/0] via 10.1.130.253
S       10.1.2.0 [1/0] via 10.1.128.252
C       10.1.1.0 is directly connected, Ethernet0
C       10.1.130.0 is directly connected, Serial1
C       10.1.128.0 is directly connected, Serial0
Albuquerque#ping 10.1.128.252

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.128.252, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

! Note: the following extended ping command will result in some debug messages
! on Yosemite in Example 5-7.

Albuquerque#ping
Protocol [ip]:
Target IP address: 10.1.2.252
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.251
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.1.2.252, timeout is 2 seconds:
. . . . .
Success rate is 0 percent (0/5)
Albuquerque#
```

Ejemplo 3.10 show ip ruote en Yosemite, Después de Agregar las rutas estáticas a Albuquerque

```
Yosemite#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

     10.0.0.0/24 is subnetted, 3 subnets
C       10.1.2.0 is directly connected, Ethernet0
C       10.1.129.0 is directly connected, Serial1
C       10.1.128.0 is directly connected, Serial0
Yosemite#ping 10.1.128.251

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.128.251, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
Yosemite#ping 10.1.1.251

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.251, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Yosemite#debug ip icmp
ICMP packet debugging is on
Yosemite#
Yosemite#show debug
Generic IP:
  ICMP packet debugging is on
Yosemite#

!NOTE: the following debug messages are a result of the extended ping
!command issued on Albuquerque in Example 5-6;
!these messages are generated by Yosemite!

ICMP: echo reply sent, src 10.1.2.252, dst 10.1.1.251
ICMP: echo reply sent, src 10.1.2.252, dst 10.1.1.251
ICMP: echo reply sent, src 10.1.2.252, dst 10.1.1.251
ICMP: echo reply sent, src 10.1.2.252, dst 10.1.1.251
ICMP: echo reply sent, src 10.1.2.252, dst 10.1.1.251
```

Los comandos ping de Cisco usan el resultado de la dirección IP de la interfase, como la dirección fuente del paquete, a menos que, por otra parte se especifique en un ping extendido. El primer ping en el ejemplo 3.9 usa una fuente de 10.1.128.251; el ping extendido usa la dirección fuente mostrada (10.1.1.251).

La versión extendida del comando ping, puede usarse para refinar totalmente la causa subyacente del problema. De hecho, cuando un ping de un ruteador trabaja, pero un ping de un host no lo hace, los ping extendidos podrían ayudar a recrear el problema sin la necesidad de trabajar con el usuario final por teléfono. Por ejemplo, el comando ping extendido en Albuquerque envió una demanda de Eco desde 10.1.1.251 (Ethernet de Albuquerque) hacia 10.1.2.252 (Ethernet de Yosemite); ninguna contestación se recibió por Albuquerque. Normalmente, los ecos son emitidos de la dirección IP de la interfase de salida; con el uso de la opción de la dirección fuente del ping extendido, la dirección IP fuente del paquete de eco puede cambiarse. Parece que las demandas de eco ICMP se recibieron por Yosemite porque los mensajes debug en Yosemite implican que envió

las contestaciones de eco ICMP de regreso a 00.1.1.251. En alguna parte entre Yosemite creando las contestaciones de eco ICMP y Albuquerque recibiéndolas, ocurrió un problema

Examinando los pasos después de que las contestaciones de eco se crearon por Yosemite, se necesita entender el problema en este ejemplo. ICMP le pregunta al software IP en Yosemite para entregar los paquetes. El código IP realiza la revisión de la tabla de ruteo IP para encontrar la ruta correcta para estos paquetes cuyo destino es 10.1.1.251. Sin embargo, el resultado del comando **show ip route** en el ejemplo 3.10 muestra que Yosemite no tiene ninguna ruta hacia la subred 10.1.1.0. Parece que Yosemite creó los mensajes de contestaciones de Eco, pero no los envió porque no tiene ninguna ruta a 10.1.1.0/24. Éste es simplemente un ejemplo en que la ruta en una dirección está trabajando bien, pero la ruta en la dirección opuesta no es.

Otras opciones para el comando ping extendido, también son bastante útiles. El bit no Fragmentar (DF) puede establecerse, junto con la cantidad de datos para enviar en el eco, para que el MTU para que toda la ruta pueda descubrirse a través de la experimentación. Los paquetes de eco que son demasiado grande para pasar sobre un enlace debido a las restricciones de MTU serán descartados, ya que el bit DF esta establecido. El valor del intervalo, puede ser establecido para que el comando ping espere mucho mas tiempo que los 2 segundos predefinidos, antes de pensar que un eco recibirá una contestación. Además, no sólo puede ser establecido un solo tamaño de Eco ICMP, pero puede usarse un rango de tamaño para dar un juego más realista de paquetes.

Una clave para resolver problemas con el comando ping, está en comprender los diferentes códigos que el comando usa, para darle un significado a las varias respuestas que se pueden recibir.
La tabla 3.5 lista varios códigos que el comando ping del IOS de Cisco puede proporcionar.

Tabla 3.5 Explicación de los Códigos que el comando ping Recibe en respuesta a su demanda de eco ICMP

Código del comando ping	Explicación
!	Respuesta de eco ICMP recibida
.	Nada se recibió
U	ICMP inalcanzable (destino) recibido
N	ICMP inalcanzable (red) recibido
P	ICMP inalcanzable (puerto) recibido
Q	ICMP fuente apagada recibida
M	No se puede fragmentar ICMP mensaje recibido
?	Paquete desconocido recibido

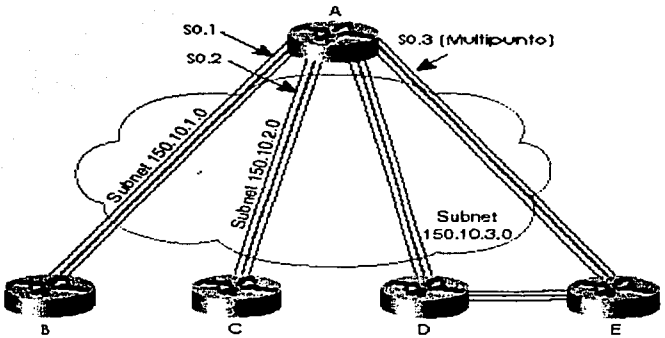
3.4.1. Direccionamiento IP con subinterfases Frame Relay

La configuración de Frame Relay puede lograrse con o sin el uso de subinterfases. Si no se usan las subinterfases, entonces todas las interfases anexas a esta misma nube Frame Relay, deberían ser configuradas con direcciones IP en la misma subred. En otros términos, se debe considerar la nube Frame Relay como cualquier otro medio de multiacceso (como una LAN). Sin embargo, la configuración Frame Relay sin subinterfases presenta algunos problemas de protocolo de ruteo cuando no hay una malla completa de circuitos virtuales (VCs) entre cada par de ruteadores. Las subinterfases le permiten a los protocolos de ruteo que funcionen bien, ya que los circuitos virtuales individuales (VCs) pueden ser considerados como interfaces separadas. Esto le permite al protocolo de ruteo mantener su característica de dividido para vencer las vueltas de ruteo.

El uso de subinterfases y el tipo de subinterfase implica el número de subredes usadas para Frame Relay. Una subinterfase punto a punto que termina en un VC y tiene una dirección IP asignada a él;

el ruteador en el otro extremo del VC, usa una dirección IP en la misma subred. Estas dos direcciones IP son las únicas dos direcciones en la subred. Cada caso separado de par de ruteadores en extremos opuestos de un VC, con una configuración de subinterfase de punto a punto, implica el uso de todavía otra subred, con sólo dos direcciones de host en la subred. El no usar subinterfases y el uso de subinterfases multipunto, es idéntico desde la perspectiva de cómo asignar las direcciones IP. Se usan las subinterfases Multipunto cuando los circuitos virtuales múltiples terminan en la subinterfase: esta subinterfase, junto con todas las subinterfases en otros ruteadores en el otro extremo de estos circuitos virtuales, son configurados para estar en la misma subred. Para cuando no se usan subinterfases, todos los ruteadores anexos a la red Frame Relay también están considerados en la misma subred. Se usan más a menudo, las subinterfases punto a punto cuando se usa una malla de circuitos virtuales. Recíprocamente, las redes multipunto se usan cuando se usa una malla completa. Sin embargo, ambos tipos de subinterfases se permiten en el mismo ruteador. La figura 3.3 muestra una configuración Frame Relay requiriendo tres subredes diferentes sobre una nube Frame Relay.

Figura 3.3 Subredes Frame Relay con subinterfases punto a punto y Multipunto



Los ejemplos 3.11, 5-10, y 3.13 muestran las configuraciones en los ruteadores A, B, y E, respectivamente.

Ejemplo 3.11 Configuración del ruteador A

```
hostname routerA
interface serial 0
encapsulation frame-relay
!
interface serial 0.1 point-to-point
ip address 150.10.1.250   255.255.255.0
frame-relay interface-dlci 40
description this is for the VC to site B
!
interface serial 0.2 point-to-point
ip address 150.10.2.250   255.255.255.0
frame-relay interface-dlci 41
description this is for the VC to site C
!
interface serial 0.3 multipoint
ip address 150.10.3.250   255.255.255.0
interface-dlci 42
interface-dlci 43
description this is for the VC's to sites D and E
```

Ejemplo 3.12 Configuración del ruteador B

```
hostname routerB
!
interface serial 0
encapsulation frame-relay
!
interface serial 0.1 point-to-point
ip address 150.10.1.251   255.255.255.0
frame-relay interface-dlci 44
description this is for the VC to site A
```

Ejemplo 3.13 Configuración del ruteador E

```
hostname routerE
!
interface serial 0
encapsulation frame-relay
!
interface serial 0.3 multipoint
ip address 150.10.3.254   255.255.255.0
frame-relay interface-dlci 44
description this is for the VC to site A
```

3.5. Configuración IPX

La tabla 3.5 y 3.6 resumen los comandos más populares usados para la configuración IPX y su comprobación.

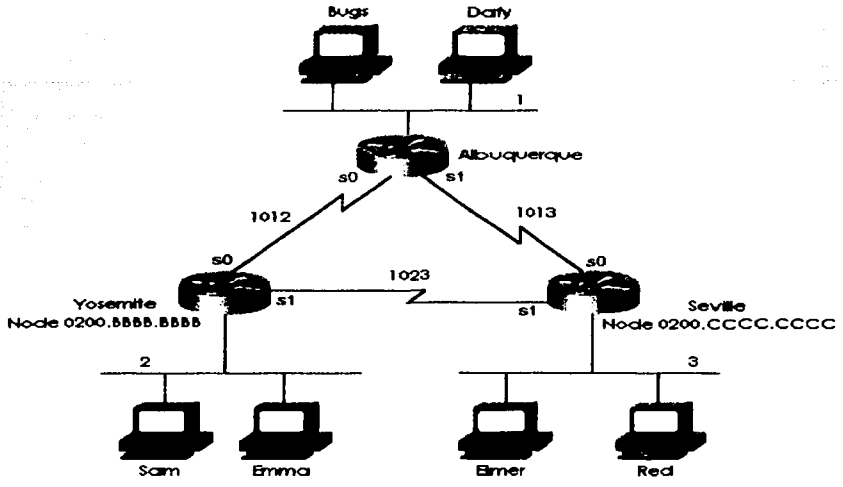
Tabla 3.5 Comandos de configuración IPX e IPX RIP

Comando	**Modo de configuración**
ipx routing [*nodo*]	Global
ipx maximum-paths *rutas*	Global
ipx network *red* [**encapsulation** *tipo*][**secondary**]	Modo Interfase

Tabla 3.6 Comandos EXEC IPX

Comando	Modo de configuración
show ipx interface	Da una vista detallada de parámetros de configuración IPX, por interfase
show ipx route [*network*]	Muestra toda la tabla de ruteo, o una entrada si en la red es introducida
show ipx servers	Muestra la tabla SAP
show ipx traffic	Muestra estadísticas de tráfico IPX
debug ipx routing [*events* | *activity*]	Muestra mensajes describiendo cada actualización de ruteo
debug ipx sap [*events* | *activity*]	Muestra mensajes describiendo cada actualización SAP
ping *ipx-address*	Envía mensajes IPX para verificar la conectividad

Figura 3.4 Red IPX con enlaces seriales punto a punto



Ejemplo 3.14 Configuración de Albuquerque para IPX, Muestra 1

```
ipx routing
!
interface serial0
ip address 10.1.12.1 255.255.255.0
ipx network 1012
bandwidth 56
!
interface serial1
ip address 10.1.13.1 255.255.255.0
ipx network 1013
!
interface ethernet 0
ip address 10.1.1.1 255.255.255.0
ipx network 1
```

Ejemplo 3.15 Configuración de Yosemite para IPX, Muestra 1

```
ipx routing 0200.bbbb.bbbb
!
interface serial0
ip address 10.1.12.2 255.255.255.0
ipx network 1012
bandwidth 56
!
interface serial1
ip address 10.1.23.2 255.255.255.0
ipx network 1023
!
interface ethernet 0
ip address 10.1.2.2 255.255.255.0
ipx network 2
```

Ejemplo 3.16 Configuración de Seville para IPX, Muestra 1

```
ipx routing 0260.cccc.cccc
!
interface serial0
ip address 10.1.13.3 255.255.255.0
ipx network 1013
!
interface serial1
ip address 10.1.23.3 255.255.255.0
ipx network 1023
!
interface ethernet 0
ip address 10.1.3.3 255.255.255.0
ipx network 3
```

La primera muestra es una configuración básica para la red en la figura 3.4. Los ejemplos 3.14, 3.15 y 3.16 proporcionan la configuración.

Nota Las muestras IPX contienen también la configuración IP. Esto no se requiere para el funcionamiento correcto de IPX. Sin embargo, para establecer una conexión de telnet hacia los ruteadores, IP debe ser configurado para emitir los comandos. De hecho, en casi cualquier red con ruteadores de Cisco, se configura IP. Por consiguiente, los ejemplos IPX generalmente incluyen la configuración de IP.

Habilitando el ruteo IPX global, así como también en cada interfase, es todo lo que se requiere para implementar el ruteo IPX en un ruteador Cisco. El comando **ipx routing** habilita el IPX en este ruteador e inicializa los procesos RIP y SAP. Los comandos individuales en cada interfase, habilitan el ruteo IPX dentro y fuera de cada interfase y habilita RIP y SAP en cada interfase, respectivamente.

Las direcciones IPX no se definen completamente, sin embargo, sólo el número de red se configura. El número completo de red IPX, se crea agregando la dirección MAC de cada interfase para el número de red IPX configurado. Para las interfaces no LAN, las direcciones MAC de una interfase LAN se usan predeterminadamente. Sin embargo, para arreglar los problemas más fácilmente, puede configurarse una dirección MAC a ser usada como parte del nodo de la dirección IPX en las interfaces no LAN. Nótese la diferencia en los dos comandos en Ejemplo 3.17. El primero está en Albuquerque, y el segundo está en Seville:

Ejemplo 3.17 show ipx interface serial 0 en Albuquerque y Seville

```
Albuquerque#show ipx interface serial 0
Serial0 is up, line protocol is up
  IPX address is 1012.0000.0ccf.21cd [up]
  Delay of this IPX network, in ticks is 6 throughput 0 link delay 0
  IPXWAN processing not enabled on this interface.
  IPX SAP update interval is 1 minute(s)
  IPX type 20 propagation packet forwarding is disabled
  Incoming access list is not set
  Outgoing access list is not set
  IPX helper access list is not set
  SAP GNS processing enabled, delay 0 ms, output filter list is not set
  SAP Input filter list is not set
  SAP Output filter list is not set
  SAP Router filter list is not set
  Input filter list is not set
  Output filter list is not set
  Router filter list is not set
  Netbios Input host access list is not set
  Netbios Input bytes access list is not set
  Netbios Output host access list is not set
  Netbios Output bytes access list is not set
  Updates each 60 seconds, aging multiples RIP: 3 SAP: 3
  SAP interpacket delay is 55 ms, maximum size is 480 bytes
  RIP interpacket delay is 55 ms, maximum size is 432 bytes
  Watchdog processing is disabled, SPX spoofing is disabled, idle time 60
  IPX accounting is disabled
  IPX fast switching is configured (enabled)
  RIP packets received 39, RIP packets sent 44
  SAP packets received 27, SAP packets sent 29
Albuquerque#


Seville#show ipx interface serial 0
Serial0 is up, line protocol is up
  IPX address is 1013.0200.cccc.cccc [up]
  Delay of this IPX network, in ticks is 6 throughput 0 link delay 0
  IPXWAN processing not enabled on this interface.
  IPX SAP update interval is 1 minute(s)
  IPX type 20 propagation packet forwarding is disabled
  Incoming access list is not set
  Outgoing access list is not set
  IPX helper access list is not set
  SAP GNS processing enabled, delay 0 ms, output filter list is not set
  SAP Input filter list is not set
  SAP Output filter list is not set
  SAP Router filter list is not set
  Input filter list is not set
  Output filter list is not set
  Router filter list is not set
```

El comando **show ipx interface** proporciona mucha información sobre IPX, incluyendo la dirección IPX completa. En este caso, se puede ver que la parte del nodo de la dirección IPX de Seville, es fácilmente reconocible, considerando que la de Albuquerque no lo es. La dirección del nodo de Seville es 0200.cccc.cccc basado en su comando de configuración **ipx routing 0200.cccc.cccc** (refiérase al Ejemplo 3.16). Sin embargo, ya que el parámetro del nodo se omitió del comando **ipx routing** en Albuquerque (refiérase al Ejemplo 3.14), el ruteador escoge una MAC en una de las interfaces LAN para usarla como la porción del nodo de la dirección IPX en las interfaces no LAN.

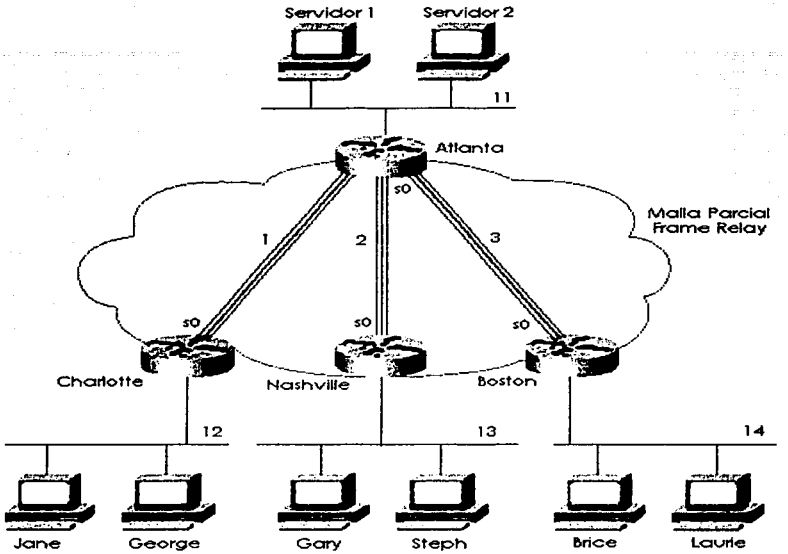
Ejemplo 3.17 show ipx interfase serial 0 en Albuquerque y Sevile (continuación)

```
  Netbios Input host access list is not set
  Netbios Input bytes access list is not set
  Netbios Output host access list is not set
  Netbios Output bytes access list is not set
  Updates each 60 seconds, aging multiples RIP: 3 SAP: 3
  SAP interpacket delay is 55 ms, maximum size is 480 bytes
  RIP interpacket delay is 55 ms, maximum size is 432 bytes
  Watchdog processing is disabled, SPX spoofing is disabled, idle time 60
  IPX accounting is disabled
  IPX fast switching is configured (enabled)
  RIP packets received 51, RIP packets sent 51
  SAP packets received 2, SAP packets sent 28
Seville#
```

Nota Después de que el comando **Ipx routing** se introduce, el ruteador salva el comando con el valor del nodo. En otros términos, aun cuando la configuración de Albuquerque se haya tecleado como en el ejemplo 3.18, el número del nodo escogido de una interfase LAN se mostraría al final del comando **Ipx routing** cuando se este viendo la configuración en el futuro.

Muchas variantes están involucradas en cómo las partes del nodo de las direcciones se asignan. El primero es, que si la parte del nodo de la dirección IPX en las interfaces WAN son derivadas de una MAC de la interfase LAN, y si hay más de una interfase LAN, entonces el IOS debe escoger una dirección MAC para usar. El algoritmo usa las direcciones MAC de la "primer" interfase Ethernet, o la primera interfase Token Ring, si no existe Ethernet, o la primera interfase FDDI, si no existen Ethernet o Token Ring. Se considera que el número de interfase numerada más bajo será el "primero". La siguiente opción es que si no existe ninguna interfase LAN, debe configurarse el parámetro del nodo en el comando **Ipx routing**, o el ruteo IPX no trabajará en una interfase WAN. La última variante es que la parte del nodo de las direcciones IPX en las interfaces LAN del ruteador, ignora el parámetro del nodo del comando **Ipx routing**, y usa su dirección MAC específica como la parte del nodo de la dirección.

Figura 3.5 Red IPX con subinterfases Frame Relay y Punto a punto



Ejemplo 3.18 Configuración de Atlanta

```
ipx routing 0200.aaaa.aaaa
!
interface serial0
encapsulation frame-relay
!
interface serial 0.1 point-to-point
ip address 140.1.1.1  255.255.255.0
ipx network 1
frame-relay interface-dlci 52
!
interface serial 0.2 point-to-point
ip address 140.1.2.1 255.255.255.0
ipx network 2
frame-relay interface-dlci 53
!
interface serial 0.3 point-to-point
ip address 140.1.3.1 255.255.255.0
ipx network 3
frame-relay interface-dlci 54
!
interface ethernet 0
ip address 140.1.11.1 255.255.255.0
ipx network 11
```

Ejemplo 3.19 Configuración de Charlotte

```
ipx routing 0200.bbbb.bbbb
!
interface serial0
encapsulation frame-relay
!
interface serial 0.1 point-to-point
ip address 140.1.1.2  255.255.255.0
ipx network 1
frame-relay interface-dlci 51
!
interface ethernet 0
ip address 140.1.12.2 255.255.255.0
ipx network 12
```

Ejemplo 3.20 Configuración de Nashville

```
ipx routing 0200.cccc.cccc
!
interface serial0
encapsulation frame-relay
!
interface serial 0.2 point-to-point
ip address 140.1.2.3 255.255.255.0
ipx network 2
frame-relay interface-dlci 51
!
interface ethernet 0
ip address 140.1.13.3 255.255.255.0
ipx network 13
```

Ejemplo 3.21 Configuración de Boston

```
ipx routing 0200.dddd.dddd
!
interface serial0
encapsulation frame-relay
!
interface serial 0.3 point-to-point
ip address 140.1.3.4 255.255.255.0
ipx network 3
frame-relay interface-dlci 51
!
interface ethernet 0
ip address 140.1.14.4  255.255.255.0
ipx network 14
```

La configuración es muy similar a la de red punto a punto de la figura 3.5. La diferencia más grande es que cada subinterfase punto a punto, es una red IPX diferente, como se vio en figura 3.6. Por otra parte, se habilita SAP y RIP globalmente con el comando **ipx routing**; cada uno se le permite ser la transmisión en las interfaces (o subinterfases) con el subcomando de interfase **ipx network**. Las actualizaciones SAP y RIP se envían fuera a cada subinterfase, esto significa, que Atlanta reproduzca y envíe tres copias de la actualización RIP y tres copias de la actualización SAP en su interfase serial 0, uno por subinterfase, cada 60 segundos.

La configuración es muy similar a la red punto a punto de la figura 3.5, La diferencia más grande es que cada subinterfase punto a punto es una red IPX diferente, como se vio en la figura 3.6. Por otra parte, se habilitan SAP y RIP globalmente con el comando **ipx routing**; a cada uno se les esta permitido ser la transmisión (broadcast) en la interfase (o subinterfases) con el subcomando de la

interfase **ipx network**. Las actualizaciones SAP y RIP son enviados fuera de cada subinterfase, esto significa que Atlanta reproduzca y envíe tres copias de la actualización RIP y tres copias de la actualización SAP en su interfase serial 0, uno por subinterfase, cada 60 segundos.

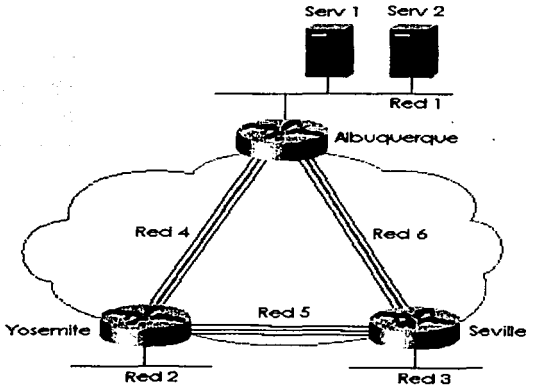
La configuración cuando se usan múltiples encapsulamientos Ethernet, es la opción de configuración final en ser repasada. En la figura 3.6, se debe asumir que Gary es un cliente NetWare viejo que corre la versión de software NetWare 3.11 y usa la encapsulamiento Ethernet 802.3 de Novell.
Stephanie es nueva y usa el encapsulamiento Ethernet 802.2. En este caso se usan dos redes IPX en la interfase Ethernet 0 de Nashville.
Gary estará en la red 13, y Stéphanie estará en la red 23. El ejemplo 3.22 muestra simplemente la configuración Ethernet para la red de Nashville, con una red IPX secundaria en la interfase Ethernet 0. El ejemplo 3.22 también muestra una configuración alternativa usando subinterfases.

Ejemplo 3.22 Configuración de Nashville con red secundaria IPX en Ethernet 0

```
ipx routing 0200.cccc.cccc

!
interface ethernet 0

ipx network 13 encapsulation novell-ether
ipx network 23 encapsulation sap secondary
! Or instead of the previous 3 lines, use the following 4 lines:
interface ethernet 0.1
ipx network 13 encapsulation novell-ether
interface ethernet 0.2
ipx network 23 encapsulation sap
```

El ejemplo 3.23 muestra el resultado de los **comandos debug ipx sap events y debug ipx routing events**. La red en la figura 3.6 fue usada para recoger el resultado de muestra.

Figura 3.6 Red de muestra usada para los comandos debug IPX



Ejemplo 3.23 Comandos debug IPX

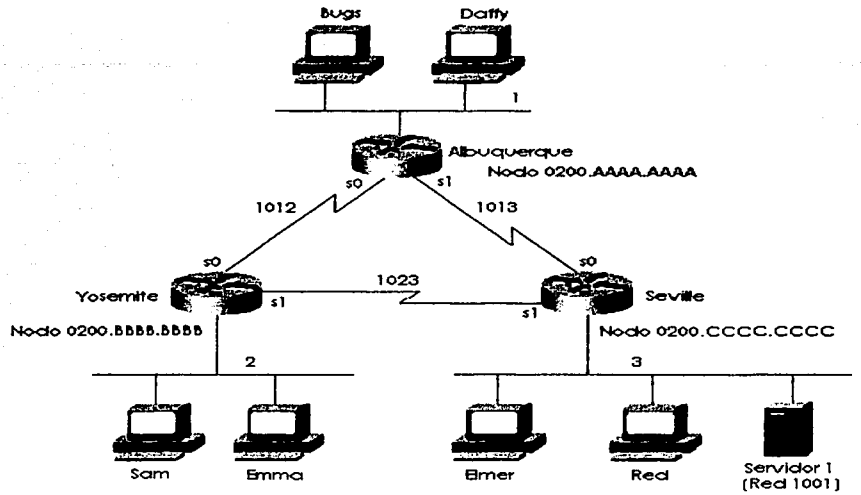
```
01:04:14: IPXRIP: 6 FFFFFFFF not added, entry in table is static/connected/internal
01:04:14: IPXRIP: positing full update to 5.ffff.ffff.ffff via Serial0.2
(broadcast)
01:04:20: IPXRIP: positing full update to 3.ffff.ffff.ffff via Ethernet0
(broadcast)
01:05:03: IPXRIP: 5 FFFFFFFF not added, entry in table is static/connected/internal
01:05:11: IPXRIP: positing full update to 6.ffff.ffff.ffff via Serial0.1
(broadcast)
01:05:14: IPXRIP: 6 FFFFFFFF not added, entry in table is static/connected/internal
01:05:14: IPXRIP: positing full update to 5.ffff.ffff.ffff via Serial0.2
(broadcast)
01:05:20: IPXRIP: positing full update to 3.ffff.ffff.ffff via Ethernet0
(broadcast)
Seville#debug ipx routing activity
IPX routing debugging is on
Seville#
01:07:02: IPXRIP: update from 6.0200.aaaa.aaaa
01:07:02: IPXRIP: 5 FFFFFFFF not added, entry in table is static/connected/internal
01:07:02:      5 in 2 hops, delay 13
01:07:02:      200 in 2 hops, delay 8
01:07:02:      11 in 3 hops, delay 8
01:07:02:      22 in 3 hops, delay 8
01:07:02:      1 in 1 hops, delay 7
01:07:02:      2 in 2 hops, delay 13
01:07:02:      4 in 1 hops, delay 7
01:07:10: IPXRIP: positing full update to 6.ffff.ffff.ffff via Serial0.1
(broadcast)
01:07:10: IPXRIP: Update len 64 src=6.0200.cccc.cccc, dst=6.ffff.ffff.ffff(453)
01:07:10:      network 3, hops 1,  delay 7
01:07:10:      network 4, hops 2,  delay 13
01:07:10:      network 2, hops 2,  delay 13
01:07:10:      network 5, hops 1,  delay 7
01:07:13: IPXRIP: positing full update to 5.ffff.ffff.ffff via Serial0.2
(broadcast)
01:07:13: IPXRIP: Update len 80 src=5.0200.cccc.cccc, dst=5.ffff.ffff.ffff(453)
01:07:13:      network 1, hops 2,  delay 13
01:07:13:      network 22, hops 4,  delay 14
01:07:13:      network 11, hops 4,  delay 14
01:07:13:      network 200, hops 3,  delay 14
01:07:13:      network 3, hops 1,  delay 7
01:07:13:      network 6, hops 1,  delay 7
01:07:13: IPXRIP: update from 5.0200.bbbb.bbbb
01:07:13: IPXRIP: 6 FFFFFFFF not added, entry in table is static/connected/internal
01:07:13:      6 in 2 hops, delay 13
01:07:13:      22 in 4 hops, delay 14
01:07:13:      11 in 4 hops, delay 14
01:07:13:      200 in 3 hops, delay 14
01:07:13:      1 in 2 hops, delay 13
01:07:13:      2 in 1 hops, delay 7
01:07:13:      4 in 1 hops, delay 7
```

```
Seville#undebug all
All possible debugging has been turned off

Seville#show ipx servers
Codes: S - Static, P - Periodic, E - EIGRP, N - NLSP, H - Holddown, + = detail
U - Per-user static
4 Total IPX Servers

Table ordering is based on routing and server info

   Type Name                          Net      Address    Port      Route Hops Itf
P     4 SVR1                         200.0000.0000.0001:0452       8/02   3  Se0.1
P     4 SVR2                         200.0000.0000.0001:0452       8/02   3  Se0.1
P     7 SVR1                         200.0000.0000.0001:0452       8/02   3  Se0.1
P     7 SVR2                         200.0000.0000.0001:0452       8/02   3  Se0.1
Seville#debug ipx sap activity
IPX service debugging is on
Seville#
00:13:21: IPXSAP: Response (in) type 0x2 len 288 src:6.0200.aaaa.aaaa
dest:6.ffff.ffff.ffff(452)
00:13:21:  type 0x4, "SVR2", 200.0000.0000.0001(452), 3 hops
00:13:21:  type 0x4, "SVR1", 200.0000.0000.0001(452), 3 hops
00:13:21:  type 0x7, "SVR2", 200.0000.0000.0001(452), 3 hops
00:13:21:  type 0x7, "SVR1", 200.0000.0000.0001(452), 3 hops
00:13:27: IPXSAP: positing update to 6.ffff.ffff.ffff via Serial0.1 (broadcast)
(full)
00:13:27: IPXSAP: suppressing null update to 6.ffff.ffff.ffff
Seville#
Seville#
00:13:30: IPXSAP: Response (in) type 0x2 len 288 src:5.0200.bbbb.bbbb
dest:5.ffff.ffff.ffff(452)
00:13:30:  type 0x7, "SVR1", 200.0000.0000.0001(452), 4 hops
00:13:30:  type 0x7, "SVR2", 200.0000.0000.0001(452), 4 hops
00:13:30:  type 0x4, "SVR1", 200.0000.0000.0001(452), 4 hops
00:13:30:  type 0x4, "SVR2", 200.0000.0000.0001(452), 4 hops
undebug all
All possible debugging has been turned off
Seville#
```

El comando **debug ipx SAP events** lista los detalles de cada actualización SAP recibida y enviada. Nótese que se muestra el número de brincos hacia el servidor, como es el tipo de servicio y el nombre del servidor. También se listan la fuente y el destino de los paquetes de actualización. El comando **debug ipx routing activity** solo lista la información resumida sobre las actualizaciones de ruteo, considerando que el comando **debug ipx routing activity** de los detalles.

El comando **ipx routing** habilita los RIP y SAP en un ruteador, y el comando **ipx network** en una interfase implica que las actualizaciones RIP y SAP deben enviarse para y escucharse en esas interfaces. El ruteador Yosemite se ha configurado para RIP y SAP (vea la figura 3.7). El comando **output** en el ejemplo 3.24, muestra el resultado de algunos comandos **Show** y **debug** de RIP y SAP.

Figura 3.7 Red IPX con enlaces seriales punto a punto



Ejemplo 3.24 Información SAP y de ruteo en Yosemite

```
Yosemite#show ipx route
Codes: C - Connected primary network,     c - Connected secondary network
       S - Static, F - Floating static, L - Local (internal), W - IPXWAN
       R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate
       s - seconds, u - uses

7 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.

No default route known.

C          2 (SAP),           E0
C       1012 (HDLC),          Se0
C       1023 (HDLC),          Se1
R          1 [07/01] via     1012.0000.aaaa.aaaa,   14s, Se0
```

```
R           3 [07/01] via      1023.0200.cccc.cccc,     1s, Se1
R        1001 [08/03] via      1023.0200.cccc.cccc,     1s, Se1
R        1013 [12/01] via      1023.0200.cccc.cccc,     1s, Se1
Yosemite#show ipx servers
Codes: S - Static, P - Periodic, E - EIGRP, N - NLSP, H - Holddown, + = detail
1 Total IPX Servers

Table ordering is based on routing and server info

   Type Name                          Net      Address   Port     Route Hops Itf
P      4 Server1                    1001.0000.0000.0001:0451       8/03   3  Se1

Yosemite#debug ipx routing activity
IPX routing debugging is on

Yosemite#
IPXRIP: positing full update to 2.ffff.ffff.ffff via Ethernet0 (broadcast)
IPXRIP: src=2.0200.bbbb.bbbb, dst=2.ffff.ffff.ffff, packet sent
    network 1, hops 2,  delay 8
    network 1001, hops 4,  delay 9
    network 1012, hops 1,  delay 2
    network 3, hops 2,  delay 8
    network 1013, hops 2,  delay 8
    network 1023, hops 1,  delay 2

IPXRIP: positing full update to 1012.ffff.ffff.ffff via Serial0 (broadcast)
IPXRIP: src=1012.0200.bbbb.bbbb, dst=1012.ffff.ffff.ffff, packet sent
    network 1001, hops 4,  delay 14
    network 3, hops 2,  delay 13
    network 1013, hops 2,  delay 13
    network 1023, hops 1,  delay 7
    network 2, hops 1,  delay 7

IPXRIP: update from 1012.0200.aaaa.aaaa
    1013 in 1 hops, delay 7
    1 in 1 hops, delay 7
    1001 in 4 hops, delay 14
    3 in 2 hops, delay 13
IPXRIP: 1023 FFFFFFFF not added, entry in table is static/connected/internal
    1023 in 2 hops, delay 13

IPXRIP: update from 1023.0200.cccc.cccc
    1 in 2 hops, delay 13
    1001 in 3 hops, delay 8
    3 in 1 hops, delay 7
    1013 in 1 hops, delay 7
IPXRIP: positing full update to 1023.ffff.ffff.ffff via Serial1 (broadcast)
IPXRIP: src=1023.0200.bbbb.bbbb, dst=1023.ffff.ffff.ffff, packet sent
    network 1, hops 2,  delay 13
    network 1012, hops 1,  delay 7
    network 2, hops 1,  delay 7
```

```
Yosemite#debug ipx sap activity
IPX service debugging is on

IPXSAP: positing update to 1012.ffff.ffff.ffff via Serial0 (broadcast) (full)
IPXSAP: Update type 0x2 len 96 src:1012.0200.bbbb.bbbb
dest:1012.ffff.ffff.ffff(452)
 type 0x4, "Server1", 1001.0000.0000.0001(451), 4 hops

IPXSAP: Response (in) type 0x2 len 96 src:1012.0200.aaaa.aaaa
dest:1012.ffff.ffff.ffff(452)
 type 0x4, "Server1", 1001.0000.0000.0001(451), 4 hops

IPXSAP: positing update to 1023.ffff.ffff.ffff via Serial1 (broadcast) (full)
IPXSAP: suppressing null update to 1023.ffff.ffff.ffff
IPXSAP: Response (in) type 0x2 len 96 src:1023.0200.cccc.cccc
dest:1023.ffff.ffff.ffff(452)
 type 0x4, "Server1", 1001.0000.0000.0001(451), 3 hops

IPXSAP: positing update to 2.ffff.ffff.ffff via Ethernet0 (broadcast) (full)
IPXSAP: Update type 0x2 len 96 src:2.0000.3089.b170 dest:2.ffff.ffff.ffff(452)
 type 0x4, "Server1", 1001.0000.0000.0001(451), 4 hops
```

Algunas de las porciones más importantes del resultado se resaltan en el ejemplo. Estas características se describen en los próximos párrafos. El comando **show ipx route**, lista los valores métricos en corchetes; el número de tic tacs se lista antes de la cuenta de salto. El numero de segundos listados al final de cada línea para rutas deducidas RIP es el tiempo desde que la información de ruteo fue escuchada; las métricas de tic tacs se muestran solo como un numero de tic tacs, nunca como un numero de segundos. Por ejemplo, en ejemplo 3.24, Yosemite lista una ruta hacia la red 3, con los números [7,1] mostrado al lado del numero de red IPX. Siete es el numero de tic tacs, el cual en este caso es la suma de seis tic tacs para el enlace serial hacia Seville, y un tic tac para el Ethernet en Seville. El uno en los corchetes representa la cuenta de salto. El comando **show ipx servers** intencionalmente se mantuvo pequeño para este ejemplo; en muchas redes, hay miles de entradas SAP. Se listan el nombre del servidor y el tipo de SAP; el tipo de SAP será importante para los filtros SAP. Las direcciones IPX y el enchufe usado por el servidor para este servicio se listan; el enchufe puede ser importante al filtrar los paquetes IPX. Los valores métricos para la ruta hacia la red 1001 se muestran bajo la palabra "ruta". Teniendo la información de la métrica a la mano, se pueden hacer buenas opciones fácilmente para las contestaciones GNS. En ejemplo 6-21, el Servidor 1 se lista con SAP tipo 4, el cual es el servidor de archivos; su dirección IPX es 1001.0000.0000.0001, y usa un puerto IPX 0451. La ruta hacia la red 1001 tiene una métrica de ocho tic tacs y tres saltos; cuando se envían los paquetes al servidor 1, ellos envían fuera de la interfase serial 1 de Yosemite.

El comando **debug ipx routing activity** habilita el resultado describiendo cada actualización RIP enviada y recibida. El número de tic tacs en las interfaces LAN esta predefinido a 1, y en las interfaces WAN están predefinidos a 6. Aunque Albuquerque y Yosemite han codificado un parámetro de ancho de banda de 56 en el enlace serial entre ellos, y los otros enlaces se predefinen a 1.544, los tic tacs no son afectados. El subcomando de la interfase **ipx delay** *ticks* pueden usarse para cambiar la métrica para una interfase en particular.

Finalmente, el comando **debug ipx sap activity** (resaltado cerca del final del ejemplo 6-15) habilita el resultado describiendo cada actualización SAP enviada y recibida. Nótese que la actualización Yosemite quiere enviar fuera la red 1023; es tiempo para enviar una transmisión SAP, pero la actualización SAP es nula. Esto es porque el único SAP en la tabla (Servidor 1, SAP tipo 4) fue aprendida de Seville sobre la red 1023, así que Yosemite esta usando las reglas del horizonte partido para no enviar la información acerca de este SAP hacia Seville.

Sólo se permite una ruta hacia cada red en la tabla de ruteo, predeterminadamente. Mirando atrás, en el principio del ejemplo 3.24, se notará que la ruta hacia la red de 1013, métrica [7/1], apunta hacia el siguiente brinco 1023.0200.cccc.cccc (Seville), fuera de la interfase serial 1 de Yosemite. Sin embargo, 1012.0200.aaaa.aaaa (Albuquerque) esta enviando las actualizaciones RIP describiendo una ruta hacia la red 1013, con siete tic tacs y un salto en la interfase Serial 0 de Yosemite (vea el resultado RIP debug). Yosemite escucho de Seville primero; por consiguiente, solo esa ruta es incluida.

Si el comando global **ipx maximum-paths** 2 ha sido configurado en Yosemite, ambas rutas serian incluidas. Al contrario con IP, cuando dos rutas están en la tabla de ruteo IPX, ocurre el balanceo de la carga por paquete a través de estas rutas. Inclusive si se habilita el switcheo rápido.

NOTA El balanceo de la carga por paquete predefinido, usado para IPX cuando múltiples rutas hacia la misma red están en la tabla de ruteo, puede no ser deseada, ya que los paquetes pueden llegar en desorden. Teniendo el ruteador que enviar todos los paquetes hacia una dirección individual IPX sobre la misma ruta cada vez, esos paquetes deben recibirse en orden. El comando de configuración **ipx per-host-load-share** desactiva el balanceo por paquete y habilita balanceo basado en la dirección de destino. Claro, la penalización es que el tráfico no será completamente equilibrado, basado en los números de paquetes hacia cada destino

3.6. Configuración de RIP e IGRP

La práctica es la mejor manera de aprender completamente los detalles de la configuración. En lugar de eso, esta sección lista los comandos y proporciona ejemplos. Las tablas 3.7 y 3.8 resumen los comandos más populares usados para, la configuración y verificación de RIP e IGRP. Dos muestras de configuración siguen.

Tabla 3.7 Comandos de configuración IP RIP e IGRP

Comando	**Modo de configuración**
router rip	Global
router igrp *proceso de identificación*	Global
network *numero de red*	Subcomando del ruteador
passive-interface *tipo numero*	Subcomando del ruteador
maximum-paths x	Subcomando del ruteador
variance *multiplicador*	Subcomando del ruteador
traffic-share {*balanceado* | *min*}	Subcomando del ruteador

Tabla 3.8 IP RIP e IGRP EXEC

Comando	Función
show ip route [*subred*]	Muestra toda la tabla de ruteo, o una entrada si se introduce una subred
show ip protocol	Muestras los parámetros del protocolo de ruteo y los valores actuales del cronometro
debug ip rip	Emite mensajes log para cada actualización RIP
debug ip igrp transactions	Emite mensajes log con detalles de las actualizaciones IGRP
debug ip igrp events	Emite mensajes log para cada paquete IGRP
Ping	Envía y recibe mensajes de eco ICMP para verificar la conectividad
Trace	Envía una serie de ecos ICMP con valores TTL crecientes para verificar la ruta actual a un host

3.7. Configuración HDLC y PPP

Una tarea común para los expertos en redes, es habilitar un protocolo de enlace de datos de punto a punto apropiado. Con LAPB siendo la excepción. (Se debe estar seguro de configurar el mismo protocolo de enlace de datos WAN en cada extremo del enlace serial, de lo contrario, los ruteadores interpretarán mal las tramas entrantes, y el enlace no funcionara) Las tablas 3.9 y 3.10 resumen los comandos de configuración y los comandos **show** y **debug** usados para la configuración HDLC y PPP.

Tabla3.9 Comandos de configuración PPP y HDLC

Comando	Modo de configuración
encapsulation {hdlc ppp lapb}	Subcomando de la interfase
compress Predictor | stac | mppc[ignore-pfc]]	Subcomando de la interfase

Tabla 3.10 Comandos show y debug relacionados con punto a punto

Comando	Función
show interfase	Lista las estadísticas y detalles de la configuración de la interfase, incluyendo el tipo de encapsulamiento.
show compress	Lista las proporciones de compresión.
show process	Lista el proceso y la utilización de tarea. Es útil cuando se mira el incremento de la utilización debido a la compresión.

El ejemplo 3.25 lista la configuración para HDLC, seguido por la configuración cambiada para una migración a PPP. Asuma que los ruteadores A y B tengan un enlace serial conectado hacia su puerto serial 0, respectivamente.

Cambiando los encapsulamientos seriales en el modo de configuración es tramposo comparado con algunos otros comandos de configuración en un ruteador Cisco. En el ejemplo 3.25, convirtiendo de regreso a HDLC (el valor predefinido) se hace con el comando **encapsulation hdlc**, no usando un comando como **no encapsulation ppp**. Adicionalmente, cualquier otro subcomando de la interfase que son solo pertinentes a PPP, también son removidos cuando el comando **encapsulation hdlc** esta en uso

Ejemplo 3.25 Configuración para PPP y HDLC

```
Router A                          Router B

Interface serial 0                Interface serial 0
encapsulation ppp                 encapsulation ppp
.                                 .
. later, changed to...            . later, changed to...
.                                 .
interface serial 0                interface serial 0
encapsulation hdlc                encapsulation hdlc
```

El Protocolo de Control de Enlace PPP (Link Control Protocol - LCP) proporciona las características básicas sin la necesidad de tener en cuenta el protocolo de capa 3 enviado a través del enlace. Una serie de protocolos de control PPP, como el Protocolo de Control IP (IP Control Protocol - IPCP), proporciona las características para un protocolo de capa en particular para funcionar bien a través del enlace.
Solo un LCP (Link Control Protocol) se necesita por enlace, pero se necesitan múltiples protocolos de control.

Si un ruteador se configura para IPX, AppleTalk, e IP en un enlace serial PPP, el ruteador configurado para encapsulamiento PPP, automáticamente intenta plantea los protocolos de control apropiados para cada protocolo de capa 3. La tabla 3.11 resume las características de LCP las cuales realizan las funciones no específicas a una capa 3 en particular.

Tabla 3.11 Características PPP LCP

Función	Numero de la característica LCP	Descripción
Detección de error	Monitoreo de la calidad del enlace (LQM)	PPP puede bajar un enlace basado en el porcentaje de errores en el enlace. LQM intercambia las estadísticas sobre los paquetes perdidos contra los paquetes enviados en cada dirección; cuando se comparan los paquetes y bytes enviados, esto produce un porcentaje de tráfico erróneo. El porcentaje de pérdida que causa que un enlace sea desconectado, es habilitado y definido por una colocación de la configuración.
Detección de enlace doblado	Numero mágico	Usando un número mágico, los ruteadores envían mensajes entre si con un número mágico diferente. Si alguna vez recibe su propio número mágico, el enlace esta doblado. Una establecimiento de la configuración, determina si el eslabón debe deshabilitarse cuando esta doblado.
Autenticación	PAP y CHAP	Mayormente usado en los enlaces de dial, PAP y CHAP pueden ser usados para autenticar el dispositivo en el otro extremo del enlace.
Compresión	STAC y predicción	Esta es compresión por software
Soporte multilink	Multilink PPP	Los fragmentos de paquetes son balanceados de carga a través de múltiples enlaces. Esta característica se usa más a menudo con dial. La sección "Multilink PPP".

3.8. Configuración Frame Relay

La configuración Frame Relay en un ruteador de Cisco es relativamente fácil si se usan todos los valores predefinidos. La experiencia es la mejor manera de aprender totalmente los detalles de la configuración. Las tablas 3.12 y 3.13 resumen los comandos más populares usados para la configuración y verificación de Frame Relay

Tabla 3.12 Comandos de configuración Frame Relay

Comando	Modo de Configuración	Propósito
Encapsulation frame-relay [ietf | cisco]	Interfase	Define el encapsulamiento de Frame Relay que se usa en lugar de HDLC, PPP, y así sucesivamente.
frame-relay lmi-type {ansi | q933a | cisco}	Interfase	Define el tipo de mensajes de LMI enviados al switch.
Bandwidth *num*	Interfase	Envía la velocidad percibida del ruteador de la interfase. El ancho de banda se usa por algunos protocolos de ruteo para influenciar la métrica.
frame-relay map *protocol protocol-address dlci* **[payloadcompress{packet-by-packet | frf9 stac}] [broadcast] [ietf | cisco]**	Interfase	Estáticamente define un mapeo entre una dirección de capa de red y un DLCI.
Keepalive *sec*	Interfase	Define si, y que a menudo se envían los mensajes de pregunta de estado LMI y cuando se esperan.
interface serial *num.sub [pointto-point | multipoint]*	Global	Crea un subinterfase, o hace referencia de una subinterfase previamente creada.
frame-relay interface-dlci *dlci* **[ietf | cisco]**	Interfase	Define que un DLCI usado para un VC hacia otro DTE.
frame-relay payload-compress{packet-by-packet | frf9 stac}	Subcomando de la interfase	Define la compresión de la carga útil en las subinterfases de punto a punto

Tabla 3.13 Relación de los comandos EXEC Frame Relay

Comando	Función
show interface	Muestra el estado de la interfase física.
show frame-relay {pvc | map | lmi}	Muestra el estado del PVC, mapeando (trazando) (dinámica y estáticamente), y el estado del LMI.
debug frame-relay {lmi | events}	Lista los mensajes describiendo los flujos LMI (opción LMI). La opción **events** lista la información ARP inversa. Otras opciones incluyen **lapf, informationelements, ppp**, y **packet**

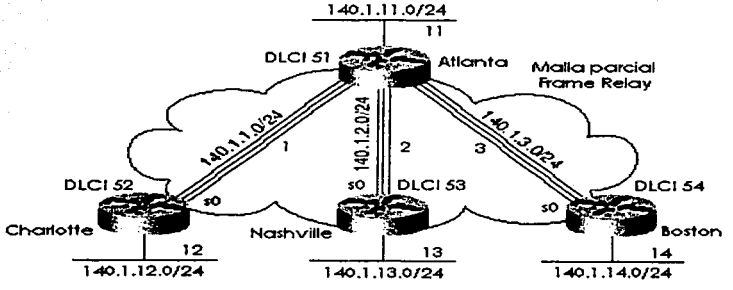
Determinar cuando y como usar las subinterfases para la configuración Frame Relay, es la parte más difícil de la configuración. Algunas pautas generales cuando se usan las subinterfases incluyen lo siguiente:

- Cuando se tiende una red parcialmente, usando subinterfases punto a punto sobrevienen problemas de horizonte partido por tratar a cada subinterfase como una interfase separada.
- Cuando la red se tiende parcialmente, funcionara usando una subinterfase multipunto.
- Cuando se tiende una red totalmente, una subinterfase multipunto puede usarse para reducir el número de grupos de capa de red (por ejemplo, subredes IP) que son usados.
- Cuando se tiende una red completamente, pueden usarse subinterfases punto a punto. Esto se escoge típicamente para mantener la consistencia con otras redes Frame Relay en otra parte en la red que no esta totalmente tendida. Esta opción requiere usar un número más grande de subredes IP.
- Cuando la red contiene varias porciones totalmente tendidas (por ejemplo, cuando 3 sitios tienen VCs entre cada uno pero los otros 10 no), una subinterfase multipunto puede usarse para la porción totalmente tendida y puede usarse subinterfases punto a punto para el resto.
- Cuando la red contiene porciones totalmente tendidas (por ejemplo, cuando 3 sitios tienen VCs entre cada uno pero los otros 10 no), solo usando subinterfases punto a punto es otra opción. Esto requiere más subredes IP y redes IPX que cuando se usa una subinterfase multipunto para la porción totalmente tendida de la red.
- Muchos sitios evitan la confusión usando siempre subinterfases punto a punto para mantener la consistencia.

3.8.1. Configurando redes con subinterfases Punto a punto

La siguiente red de muestra basada en el ambiente descrito en la figura 3.8, usa subinterfases punto a punto. Los ejemplos 3.26, 3.27, y 3.28 muestran la configuración para esta red.

Figura 3.8 Malla Parcial con direcciones IP e IPX



Ejemplo 3.26 Configuración de Atlanta

```
ipx routing 0200.aaaa.aaaa
!
interface serial0
encapsulation frame-relay
!
interface serial 0.1 point-to-point
ip address 140.1.1.1  255.255.255.0
ipx network 1
frame-relay interface-dlci 52
!
interface serial 0.2 point-to-point
ip address 140.1.2.1 255.255.255.0
ipx network 2
frame-relay interface-dlci 53
!
interface serial 0.3 point-to-point
ip address 140.1.3.1 255.255.255.0
ipx network 3
frame-relay interface-dlci 54
!
interface ethernet 0
ip address 140.1.11.1 255.255.255.0
ipx network 11
```

Ejemplo 3.27 Configuración de Charlotte

```
ipx routing 0200.bbbb.bbbb
!
interface serial0
encapsulation frame-relay
!
interface serial 0.1 point-to-point
ip address 140.1.1.2  255.255.255.0
ipx network 1
frame-relay interface-dlci 51
!
interface ethernet 0
ip address 140.1.12.2 255.255.255.0
ipx network 12
```

Ejemplo 3.28 Configuración de Nashville

```
ipx routing 0200.cccc.cccc
!
interface serial0
encapsulation frame-relay
!
interface serial 0.2 point-to-point
ip address 140.1.2.3 255.255.255.0
ipx network 2
frame-relay interface-dlci 51
!
interface ethernet 0
ip address 140.1.13.3 255.255.255.0
ipx network 13
```

En esta configuración se usaron subinterfases punto a punto, ya que la red no está tendida totalmente. El comando **frame-relay interface-dlci** se necesita al usar subinterfases. Esto es porque los mensajes de estado entran en la interfase física que declara que un VC con un DLCI en particular esta activo; el IOS necesita asociar ese VC con una subinterfase.

Los números de las subinterfases en la configuración de ejemplo están para comparar en cualquier extremo de los VCs. Por ejemplo, la subinterfase 2 fue usada en Atlanta para el PVC hacia Nashville; Nashville también usa una subinterfase 2. No hay ningún requisito para que los números de la subinterfase sean los mismos.

El ejemplo 3.29 muestra el resultado de los comandos Frame Relay EXEC del IOS más populares para monitorear Frame Relay, como se emitió en el ruteador Atlanta.

Ejemplo 3.29 Resultado de los comandos EXEC en Atlanta

```
  in BECN pkts 0             out FECN pkts 0            out BECN pkts 0
  in DE pkts 0               out DE pkts 0
  out bcast pkts 875         out bcast bytes 142417
  pvc create time 05:19:51, last time pvc status changed 04:55:41
 --More--
DLCI = 54, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0.3

  input pkts 10              output pkts 877            in bytes 1274
  out bytes 142069           dropped pkts 0             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 877          out bcast bytes 142069
  pvc creaté time 05:19:52, last time pvc status changed 05:17:42

Atlanta#show frame-relay map
Serial0.3 (up): point-to-point dlci, dlci 54(0x36,0xC60), broadcast
        status defined, active
Serial0.2 (up): point-to-point dlci, dlci 53(0x35,0xC50), broadcast
        status defined, active
Serial0.1 (up): point-to-point dlci, dlci 52(0x34,0xC40), broadcast
        status defined, active

Atlanta#debug frame-relay lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data

Serial0(out): StEnq, myseq 163, yourseen 161, DTE up
datagramstart = 0x45AED8, datagramsize = 13
FR encap = 0xFCF10309
00 75 01 01 01 03 02 A3 A1

Serial0(in): Status, myseq 163
RT IE 1, length 1, type 1
KA IE 3, length 2, yourseq 162, myseq 163
```

La información de dirección útil se llevo a cabo en el resultado del **comando show frame-relay pvc**. Los contadores para cada VC, incluyendo incrementos en los contadores FECN y BECN, pueden ser particularmente útiles. Así como también, comparar los paquetes/bytes enviados contra lo que se recibe en el otro extremo del VC también es bastante útil, porque refleja el número de paquetes/bytes perdidos dentro de la nube Frame Relay. También, viendo un PVC como activo, significa que es utilizable (como opuesto a inactivo) que es un gran lugar para empezar cuando se esta arreglando problemas. Toda esta información puede recogerse bien por un administrador SNMP.

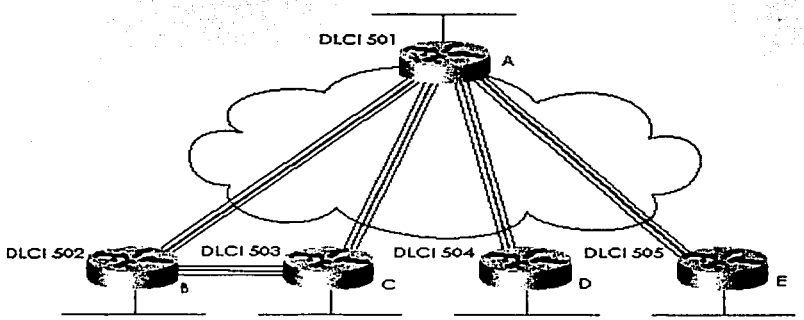
El resultado del comando **show frame-relay map** es sorprendente después del discurso acerca del mapeo. Un DLCI se lista en cada entrada, pero no se hace ninguna mención de la dirección de la capa 3 correspondiente. Sin embargo, ya que las subinterfases son punto a punto, esta omisión por el IOS es intencional, la subinterfase actúa como un enlace punto a punto, con dos participantes. El mapeo sólo se necesita cuando más de dos dispositivos se unen al enlace. (Vea la sección "Como funciona el trazado (mapeo) de dirección", anteriormente en este capítulo, para más información.)

El resultado de **debug frame-relay lmi** muestra una indicación de ambos, envío y recepción. El mensaje de estado es enviado por el switch, considerando que la pregunta de estado es enviada por el DTE (ruteador). La colocación keepalive del IOS, no causa que los paquetes fluyan entre los ruteadores, sino que causa que el ruteador envíe los mensajes LMI al switch. También causa que el ruteador espere mensajes LMI del switch.

3.8.2. Configurando redes con subinterfases coexistentes Punto .a punto y Multipunto

Las redes Frame Relay construidas por los especialistas en redes, mas probablemente incluirán subinterfases punto a punto y multipunto. Esta última red de muestra (basada en el ambiente descrito en la figura 3.9) usa ambos tipos de subinterfases. El ejemplo 3.30, 3.31, 3.32, 3.33, y 3.34 muestran la configuración para esta red.

. Figura 3.9 Híbrido de Malla completa y parcial



Ejemplo 3.30 Configuración del ruteador A

```
hostname RouterA
!
ipx routing 0200.aaaa.aaaa
!
interface serial0
encapsulation frame-relay
!
interface serial 0.1 multipoint
ip address 140.1.1.1  255.255.255.0
ipx network 1
frame-relay interface-dlci 502
frame-relay interface-dlci 503
!
interface serial 0.2 point-to-point
ip address 140.1.2.1 255.255.255.0
ipx network 2
frame-relay interface-dlci 504
!
interface serial 0.3 point-to-point
ip address 140.1.3.1 255.255.255.0
ipx network 3
frame-relay interface-dlci 505
!
interface ethernet 0
ip address 140.1.11.1 255.255.255.0
ipx network 11
```

Ejemplo 3.31 Configuración del ruteador B

```
hostname RouterB
!
ipx routing 0200.bbbb.bbbb
!
interface serial0
encapsulation frame-relay
!
interface serial 0.1 multipoint
ip address 140.1.1.2  255.255.255.0
ipx network 1
frame-relay interface-dlci 501
frame-relay interface-dlci 503
!
interface ethernet 0
ip address 140.1.12.2 255.255.255.0
ipx network 12
```

Ejemplo 3.32 Configuración del ruteador C

```
hostname RouterC
!
ipx routing 0200.cccc.cccc
!
interface serial0
encapsulation frame-relay
!
interface serial 0.1 multipoint
ip address 140.1.1.3  255.255.255.0
ipx network 1
frame-relay interface-dlci 501
frame-relay interface-dlci 502
!
interface ethernet 0
ip address 140.1.13.3 255.255.255.0
ipx network 13
```

3.33 Configuración del ruteador D

```
hostname RouterD
!
ipx routing 0200.dddd.dddd
!
interface serial0
encapsulation frame-relay
!
interface serial 0.1 point-to-point
ip address 140.1.2.4  255.255.255.0
ipx network 2
frame-relay interface-dlci 501
!
interface ethernet 0
ip address 140.1.14.4 255.255.255.0
ipx network 14
```

Ejemplo 3.34 Configuración del ruteador E

```
hostname RouterE
!
ipx routing 0200.eeee.eeee
!
interface serial0
encapsulation frame-relay
!
interface serial 0.1 point-to-point
ip address 140.1.3.5 255.255.255.0
ipx network 3
frame-relay interface-dlci 501
!
interface ethernet 0
ip address 140.1.15.5 255.255.255.0
ipx network 15
```

Ningún informe del mapeo se requirió para la configuración en el ejemplo 3.30 hasta el ejemplo 3.34, ya que ARP Inverso se habilita predefinidamente en las subinterfases multipunto. Las subinterfases punto a punto no requieren los informes de mapeo, porque después de que la subinterfase saliente se identifica, hay un sólo posible ruteador al cual remitir la trama.

El ruteador A es el único ruteador que usa ambas subinterfases multipunto y punto a punto. En la interfase serial 0.1 del ruteador A, se usa multipunto, con DLCIs para los ruteadores B y C listados. En la otras dos interfaces del ruteador A, otras dos subinterfases, las cuales son punto a punto, solo se necesita listarse un DLCI. De hecho, sólo se permite un comando **frame-relay interface-dlci** en una subinterfase punto a punto, porque sólo se permite un VC. Por otra parte, las configuraciones entre los dos tipos son similares.

El ejemplo 3.35 muestra los resultados del ARP Inverso y una copia del **debug frame-relay events** mostrando los contenidos del ARP Inverso. El **debug** en el ejemplo 3.35 proporciona una visión en el funcionamiento del ARP Inverso.

Ejemplo 3.35 Mapas Frame Relay y ARP Inversos en el ruteador C

```
RouterC#show frame-relay map
Serial0.10 (up): ip 140.1.1.1 dlci 501(0x1F5,0x7C50), dynamic,
              broadcast,, status defined, active
Serial0.10 (up): ip 140.1.1.2 dlci 502(0x1F6,0x7C60), dynamic,
              broadcast,, status defined, active
Serial0.10 (up): ipx 1.0200.aaaa.aaaa dlci 501(0x1F5,0x7C50), dynamic,
              broadcast,, status defined, active
Serial0.10 (up): ipx 1.0200.bbbb.bbbb dlci 502(0x1F6,0x7C60), dynamic,
              broadcast,, status defined, active

RouterC#debug frame-relay events
Frame Relay events debugging is on

RouterC#configure terminal
Enter configuration commands, one per line.  End with Ctrl-Z.
RouterC(config)#interface serial 0.1
```

```
RouterC(config-subif)#no shutdown
RouterC(config-subif)#^Z
RouterC#

Serial0.1: FR ARP input
Serial0.1: FR ARP input
Serial0.1: FR ARP input
datagramstart = 0xE42E58, datagramsize = 30
FR encap = 0x7C510300
80 00 00 00 08 06 00 0F 08 00 02 04 00 09 00 00
8C 01 01 01 7C 51 8C 01 01 03

datagramstart = 0xE427A0, datagramsize = 46
FR encap = 0x7C510300
80 00 00 00 08 06 00 0F 81 37 02 0A 00 09 00 00
00 00 00 01 02 00 AA AA AA AA 7C 51 00 00 00 01
02 00 CC CC CC CC 1B 99 D0 CC

datagramstart = 0xE420E8, datagramsize = 30
FR encap = 0x7C610300
80 00 00 00 08 06 00 0F 08 00 02 04 00 09 00 00
8C 01 01 02 7C 61 8C 01 01 03

Serial0.1: FR ARP input
datagramstart = 0xE47188, datagramsize = 46
FR encap = 0x7C610300
80 00 00 00 08 06 00 0F 81 37 02 0A 00 09 00 00
00 00 00 01 02 00 BB BB BB BB 7C 61 00 00 00 01
02 00 CC CC CC CC 1B 99 D0 CC
```

El comando **show frame-relay map** proporciona una visión completa en el trazado (mapeo). Las direcciones IP e IPX de los ruteadores vecinos, correlacionan a los DLCIs. Esto es posible porque los mensajes ARP inversos fluyen sobre un VC; el ARP inverso contiene un tipo de protocolo y dirección de capa 3. El DLCI pone en correlación a una subinterfase basada en la configuración.

Los mensajes acerca de ARP inverso en el resultado de **debug frame-relay events** no son tan obvios. Un ejercicio fácil es buscar la versión hexadecimal de las direcciones IP e IPX en el resultado. Estas direcciones se han resaltado en el ejemplo 3.35. Por ejemplo, los primeros 3 bytes de 140.1.1.0 son 8C 01 01 en hexadecimal; este campo empieza en el lado izquierdo del resultado, así que es fácil reconocer visualmente. La dirección IPX debe ser mucho más fácil de reconocer, porque ya está en formato hexadecimal en la configuración.

NOTA Habilitando las opciones **debug**, aumenta la utilización del CPU del ruteador. Dependiendo de cuánto procesamiento se requiere y cuántos mensajes se generan, es posible degradar el rendimiento significativamente y posiblemente colapsar el ruteador. Este es un resultado de memoria y procesamiento usado para buscar la información pedida y para procesar los mensajes. Usted podría querer teclear el comando **no debug all** primero, y después teclear el comando **debug**. Si el comando **debug** crea demasiados resultados, el comando **no debug all** puede retirarse fácilmente (presionar Ctrl+P dos veces).

Si ARP inverso no se usara en absoluto en cualquiera de los tres ruteadores, los siguientes informes **frame-relay map** se habrían requerido en el ruteador A. Comandos similares se habrían requerido en los ruteadores B y C.

3.9. Configuración de ISDN

El ejemplo 3.36 y 3.37 muestran la configuración de DDR para una red. Se han agregado los detalles de la configuración ISDN; el texto que sigue a estos dos ejemplos, describe los comandos ISDN mostrados.

Ejemplo 3.36 Configuración de SanFrancisco Completa

```
username SanFrancisco password Clark
!
interface bri 0
 encapsulation ppp
 ppp authentication chap
 isdn switch-type basic-ni1
!
router igrp 6
network 172.16.0.0
```

Los comandos de configuración ISDN se delinean en los ejemplos por medio de texto resaltado; esos comandos se describen en el siguiente texto. Por ejemplo, los tipos del switch son un parámetro requerido para la conexión a los switches DMS-100 o National ISDN; se debe preguntar al proveedor de servicio el tipo de switch en cada sitio. El enlace BRI LosAngeles se conecta a un switch National ISDN, en este caso. El tipo de switch puede configurarse con el comando **isdn switch-type**, el cual puede usarse como un comando global o con un subcomando de interfase si el ruteador se conecta hacia tipos diferentes de múltiples switches ISDN. Los SPIDs pueden no ser requeridos; ellos se usan como una forma de autenticación por el switch. Los SPIDs se configuran con subcomandos de interfase BRI en SanFrancisco. También, escondido en parte de la configuración de DDR, la velocidad del canal B de SanFrancisco hacia GothamCity será de 56 Kbps, según el parámetro de velocidad en el comando **dialer map** en SanFrancisco.

La autenticación PAP o CHAP se requiere para las conexiones de marcado ISDN BRI. Como se vio en el ejemplo 3.38, ha ocurrido una conexión de marcación DDR sobre BRI 0 de SanFrancisco hacia LosAngeles:

```
  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 total/threshold/drops)
     Conversations  0/1/256 (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
     44 packets input, 1986 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
     49 packets output, 2359 bytes, 0 underruns
     0 output errors, 0 collisions, 7 interface resets
     0 output buffer failures, 0 output buffers swapped out
     11 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up


SanFrancisco# show dialer interface bri 0

BRI0 - dialer type = ISDN

Dial String     Successes   Failures    Last called   Last status

0 incoming call(s) have been screened.

BRI0: B-Channel 1
Idle timer (300 secs), Fast idle timer (120 secs)
Wait for carrier (30 secs), Re-enable (15 secs)

Dialer state is data link layer up

Dial reason: ip (s=172.16.1.1, d=172.16.3.1)


Time until disconnect 18 secs
Current call connected 00:14:00
Connected to 14045551234 (LosAngeles)

BRI0: B-Channel 2
Idle timer (300 secs), Fast idle timer (120 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

 SanFrancisco# show isdn active
 ------------------------------------------------------------------------------
                                ISDN ACTIVE CALLS
------------------------------------------------------------------------------
History Table MaxLength = 320 entries
History Retain Timer = 15 Minutes
------------------------------------------------------------------------------
Call Calling     Called         Duration  Remote   Time until   Recorded Charges
```

```
Type Number     Number          Seconds   Name      Disconnect   Units/Currency
-------------------------------------------------------------------------------
Out             14045551234     Active(847) LosAngeles     11       u
-------------------------------------------------------------------------------


SanFrancisco# show isdn status
The current ISDN Switchtype = ntt
ISDN BRI0 interface
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 64, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        1 Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 1
        CCB:callid=8003, callref=0, sapi=0, ces=1, B-chan=1
    Number of active calls = 1
    Number of available B-channels = 1
    Total Allocated ISDN CCBs = 1


SanFrancisco# debug isdn q931
ISDN q931 protocol debugging is on
Tx -> SETUP pd = 8 callref = 0x04
 Bearer Capability i = 0x8890
 Channel ID i = 0x83
 Called Party Number i = 0x80, `14045551234'
SanFrancisco#no debug all
All possible debugging has been turned off

SanFrancisco# debug dialer events
Dialer event debugging is on
Dialing cause: BRI0: ip (s=172.16.1.1, d=172.16.3.1)
SanFrancisco#no debug all
All possible debugging has been turned off

SanFrancisco# debug dialer packets
Dialer packet debugging is on
BRI0: ip (s=172.16.1.1, d=172.16.3.1) 444 bytes, interesting (ip PERMIT)
```

Ejemplo 3.37 Configuración de LosAngeles solo recepción

```
ip route 172.16.3.0 255.255.255.0 172.16.2.1
ip route 172.16.4.0 255.255.255.0 172.16.2.3
! Added usernames for CHAP support!
username LosAngeles password Clark
username GothamCity password Bruce
!
access-list 101 permit tcp any host 172.16.3.1 eq 80
access-list 101 permit tcp any host 172.16.4.1 eq 21
!
dialer-list 2 protocol ip list 101
!
interface bri 0
 encapsulation ppp
 ppp authentication chap
 isdn spid1 555555111101
 isdn spid2 555555222202
 dialer idle-timeout 300
 dialer fast-idle 120
 dialer map ip 172.16.2.1 broadcast name LosAngeles 14045551234
 dialer map ip 172.16.2.3 broadcast speed 56 name GothamCity 1999999999901
 dialer-group 2
!
router igrp 6
network 172.16.0.0
```

Ejemplo 3.38 Comandos DDR en SanFrancisco

```
SanFrancisco# show interfaces bri 0:1

BRI0:1 is down, line protocol is down
  Hardware is BRI
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
  LCP Open
  Open: IPCP, CDPCP
  Last input 00:00:05, output 00:00:05, output hang never
```

Los valores del cronómetro actuales y la razón de la llamada de arreglo se lista por el primer comando en el ejemplo 8-32, **show dialer interface bri 0.** La llamada ha estado activa a durante 14 minutos, y 18 segundos quedan antes de que el cronómetro de inactividad de 300 segundos expirará y desactivara la conexión. El comando **show isdn** active lista el hecho de que una sola llamada activa existe hacia LosAngeles, con ahora solo 11 segundos restantes hasta que se desconecte. El comando **show isdn status** lista el tipo de switch (ntt) y lista el hecho de que una llamada esta activa, el cual deja un canal B inactivo.
Recordando la idea general detrás del resultado del comando **debug**, también es útil para los Especialistas en redes que las opciones correctas puedan habilitarse rápidamente. El comando **debug isdn q921** (no mostrado) listan los detalles del protocolo LAPD entre el ruteador y el switch ISDN. El comando **debug isdn q931** lista el resultado para la llamada de arreglo y desconectar; el resultado en el ejemplo muestra el resultado típico de lo que pasó en SanFrancisco cuando la llamada hacia LosAngeles fue hecho. Los comandos **debug dialer events** y **debug dialer packets** proporcionan la información similar cuando un paquete es un candidato por causar que la marcación ocurra, en otras palabras, cuando un paquete se enruta fuera de la interfase de marcación.

3.10. Simuladores

Para llevar a cabo las configuraciones que se requieren en la elaboración de las prácticas, solo hay dos opciones, contar con el equipo requerido (ruteadores y switches) o, en este caso el uso de simuladores. En esta tesis se propone el uso de un simulador para auxiliarse a la hora de realizar las configuraciones.
El simulador que se escogió para este caso, simula el comportamiento del sistema operativo del ruteador en detalle. Ya que se pretende llevar a cabo las configuraciones lo mas realistas posibles, para así adquirir la práctica necesaria y obtener la suficiente habilidad en la configuración de los ruteadores de Cisco.

3.10.1. ¿Que son los simuladores?

Cuando se requiere una capacitación en un área especifica, un entrenamiento en una maquinaria o aeroplano, o simplemente, cuando se necesita hacer una planeación de un proyecto, es necesario contar con el equipo necesario para ese entrenamiento o bien contar con los llamados simuladores. Por ejemplo, en el pasado, una compañía automotriz al diseñar un vehículo debía adaptar sobre la marcha los diferentes componentes mecánicos e hidráulicos ya existentes, en un nuevo diseño de chasis y carrocería, para después ver su comportamiento en la pista. Este proceso se llevaba mucho tiempo e implicaba en encarecimiento del producto, así como un resultado no muy óptimo. En la actualidad con el desarrollo de computadoras cada vez mas potentes, se cuenta con una herramienta muy importante, los simuladores, los cuales ayudan a predecir el comportamiento de los componentes mecánicos, armando el vehículo y conduciéndolo en pistas virtuales así como también simulando su comportamiento en cuestiones de enfriamiento rigidez del chasis etc, llegando a una optimización sin hacer un gasto de tiempo y dinero en exceso

Otro ejemplo quizá más común en el que se ha escuchado hablar de los simuladores, es en la industria aeronáutica, ya que la necesidad de un adecuado entrenamiento de los pilotos es vital en esta área. Los simuladores de este tipo entrenan a los nuevos pilotos o también a los pilotos experimentados cuando se introduce un nuevo tipo de aeronave.
Imaginemos por un momento si no existieran este tipo de simuladores, los pilotos tendrían que capacitarse en aviones reales, los cuales representarían un peligro y además el costo del entrenamiento seria demasiado alto, por lo que sería mas costoso el servicio.

Un simulador es un Software que emula el comportamiento de un dispositivo o un sistema los cuales pueden ser, mecánicos, eléctricos neumáticos, etc. Estos programas ayudan a determinar el comportamiento de estos dispositivos cuando por motivos de costo o disponibilidad del equipo no se cuenta con las herramientas necesarias para la capacitación.

La industria de las telecomunicaciones requiere gente capacitada para afrontar los retos que se plantean al diseñar redes de voz y datos. Ciertamente es una necesidad la constante preparación en esta área, y debido a que las principales compañías proveedoras de equipos ofrecen cursos de certificación, el entrenamiento se vuelve un poco difícil si no se tiene acceso a los dispositivos en los cuales requerimos una determinada práctica. En el área de redes de datos los simuladores de ruteadores son de gran ayuda, ya que no es posible desconectar y desconfigurar un ruteador de alguna empresa para llevar a cabo nuestras prácticas y pruebas. Además los ruteadores son bastante caros como para adquirir uno y en la comodidad de nuestro hogar hacer pruebas. Por lo anterior, los simuladores son una herramienta fundamental.

3.10.2. Simuladores de ruteadores

Existen varios programas que simulan el sistema operativo de los ruteadores, el simulador que se escogió fue el Boson Router Simulator, debido a que es el mas completo dentro de esta categoría. El cual nos ayudará a comprender y familiarizarnos con el ambiente del sistema operativo y a realizar configuraciones del mismo modo en que se llevan a cabo en los ruteadores.

3.11. Software Boson Router simulator

El simulador Boson Router Simulator fue desarrollado por ingenieros de la compañía Boson, los cuales cuentan con varias certificaciones de Cisco, como CCIP, CCDP etc. Lo que los llevó a conformar uno de los simuladores más completos para la capacitación y la preparación para los exámenes de certificación de Cisco, además de contar con el reconocimiento de Cisco Systems.

3.11.1. Características:

El simulador cuenta con una herramienta que permite el diseño gráfico de una red, la cual muestra en miniatura los dispositivos que se desean interconectar. Además de tener una barra de dispositivos, los cuales se pueden elegir el tipo de ruteador, tipo de switch, la conexión que se desea, etc.

El simulador muestra una serie de botones en la parte de la barra de herramientas, los cuales representan los dispositivos involucrados en el diseño de la red. Al presionar el botón que simula un ruteador, se puede comenzar la configuración del mismo, así como también se puede configurar los demás dispositivos que intervienen en la topología de la red, planear la numeración en cada host y decidir que tipo de conexión se va a establecer entre los dispositivos, tales como ISDN Ethernet o Serial.

También cuenta con una sección de laboratorios, la cual muestra una serie de preguntas acerca de temas específicos, los cuales nos sirven para verificar nuestro nivel de aprendizaje en el sistema operativo y sus comandos, por medio de una serie de preguntas con sus respectivas respuestas, con el objetivo de ir avanzando en los temas que se requieren para la configuración de los ruteadores.

Al iniciar el simulador, se muestra un cuadro con tres opciones, las cuales son

- Cargar el simulador usando las opciones preestablecidas
- Cargar la utilidad de diseño de red
- Cargar el simulador con una topología previamente guardada

Al iniciar el simulador en las opciones predeterminadas, lo que se puede apreciar en la pantalla es, un cuadro con cinco ruteadores, un switch y una PC. También se puede ver el icono de topología, el cual sirve para ver como está configurada la red en la cual se está trabajando, en este caso la predefinida, los enlaces que tiene y sus interfaces. Otra opción que se puede ver es la del laboratorio actual (current lab), esta sección contiene información de los comandos y de cómo utilizarlos, además de una serie de lecciones que acompaña a cada uno de los laboratorios, estas opciones son muy útiles, ya que si se tiene una duda de lo que cada comando puede hacer, estas secciones pueden consultarse en cualquier momento, cabe mencionar que esta sección es parte del software del simulador, el ruteador no cuenta con esta ayuda.

Con la opción de cargar la utilidad de diseño de red, se puede hacer diseños propios, esta opción es la misma a la que se tiene en la barra de herramientas, en la cual se puede ver la opción llamada diseñe su propia red, esta permite escoger diferentes componentes de red para hacer un diseño de red que mas nos convenga. Además permite escoger entre diferentes modelos de ruteadores y switches, ya que unos modelos cuentan con mayor versatilidad en lo que se refiere a

las interfaces, es decir, algunos modelos cuentan con mayor número de interfaces seriales, Ethernet e ISDN, o una combinación de todas.
Se puede seleccionar también le tipo de conexión que se requiera para los enlaces, entre estas opciones se tienen Ethernet, ISDN y Serial.
Cuando se elabora un diseño de red nuevo, una vez terminado, se guarda y se tiene que cerrar la aplicación para entonces elegir la opción "Cargar el simulador con una topología previamente guardada" para que al iniciar el simulador la red que se diseñó este disponible para su configuración

Seleccionando el ruteador 1 de la topología predeterminada, se puede notar que aparece una pantalla blanca, esto es por que el simulador imita el comportamiento del ruteador cuando se accesa en el, en un ruteador real se conecta desde una PC (Generalmente es una Lap top, ya que es mas fácil su traslado cuando se configuran varios ruteadores) al puerto auxiliar por medio de una interfase RJ-45 con cable cruzado. En la PC, desde Windows se selecciona en el menú de inicio, la opción de programas, accesorios, comunicaciones y después la opción de telnet. Con esto se logra la comunicación hacia el ruteador, la conexión de telnet automáticamente abre la aplicación de block de notas de Windows, por lo que las configuraciones se llevan a cabo desde esa pantalla que se muestra ingresando al ruteador. En este caso, dando un enter en la pantalla del ruteador 1, muestra el indicador siguiente:

Router>

En este modo se puede hacer uso del comando de ayuda, el cual muestra los comandos disponibles para este modo de configuración tecleando "?"
En este modo se tiene un acceso restringido al ruteador, es decir, solo de podrán usar los comandos para ver la configuración del ruteador y datos de las interfaces, sin hacer cambios, esto es de gran ayuda, ya que solo la persona autorizada para hacer los cambios puede ingresar al modo privilegiado tecleando una contraseña previamente establecida.
Para ingresar al modo privilegiado, solo de teclea el comando enable, el indicador cambiara para mostrarnos que ya estamos en el modo privilegiado y se verá de la siguiente forma:

Router#

Una vez en este modo, los comandos de configuración están disponibles y se puede proceder con las configuraciones. Se puede guardar la configuración de los ruteadores por separado o si se prefiere se puede guardar la configuración de toda la red, como si se tratara de un archivo

3.11.2. Requerimientos del sistema

La versión que se instalará es la Boson Router Simulator V 4.15, esta versión requiere que la PC en la cual se desee instalar este software tenga las siguientes características:

- Pentium 266 Mhz o superior
- CD ROM 4X
- Windows 95/98/98 SE/Me/NT/2000
- 32 MB RAM
- 15 MB de espacio libre en disco duro

Capítulo 4 Configuraciones de casos reales

Introducción

En este capítulo se muestra una visión diferente de las configuraciones y de los dispositivos involucrados, como son los ruteadores y los switches. Las configuraciones de los casos reales que se muestran en este capítulo, son solo de muestra, debido a que solo se pretende hacer una comparación de cómo se llevan a cabo en un ruteador real, además de otras características de conexión.

4.1. Acceso al ruteador

Una vez que una persona tiene acceso al ruteador, especialmente al modo privilegiado o a lo que a menudo se llama "modo habilitado", puede tomar un control completo del ruteador y de su comportamiento. Es básico en un entorno seguro que se autentique y se tenga en cuanta el acceso al "modo habilitado" en cualquier ruteador. La importancia de esto radica no sólo en quien puede controlar el comportamiento del ruteador, sino también para proteger el la información que recopila el ruteador en la red. Si una persona puede leer las configuraciones y estadísticas del ruteador, puede saber muchas cosas acerca de las directivas, topologías, patrones de tráfico, tablas de enrutamiento y los protocolos de la red. Por lo tanto, controlar quien puede acceder a un ruteador es algo más que simplemente proteger un dispositivo: es proteger la topología y el funcionamiento integrado de todos los sistemas informáticos, configuraciones y directivas. El acceso a los ruteadores de Cisco de varias maneras, por lo que se debería establecer al menos una contraseña para cada una de las siguientes cuatro condiciones:

- La contraseña de habilitación (enable)
- La contraseña de la consola.
- La contraseña de la línea terminal virtual (VTY)
- La contraseña de la línea auxiliar.

4.1.1. Puerto de la consola

Cuando se accede al por primera vez al ruteador, de forma predeterminada, no es necesaria ninguna contraseña para el acceso a la consola. Podemos cambiar esto para que no se puedan conectar las personas sin privilegios. Para hacerlo simplemente introduzca los siguientes comandos durante la configuración:

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password DiFIcilDEaDIviNArCONSOLA
```

Se debe recordar también que las configuraciones del ruteador, de forma predeterminada no necesitan contraseñas en estas líneas, no solo tienen que establecer una contraseña para ellas, sino que también debe configurar un comando **login** para ellas. Sin el comando **login**, no aparecerá la petición de la contraseña y se ignorará la contraseña.

4.1.2. Puertos VTY

Los ruteadores de Cisco no tienen configurada ninguna contraseña predeterminada en sus puertos VTY. El problema es que los ruteadores de Cisco exigen una forma ¡predeterminada que se hayan establecido las contraseñas de las líneas de VTY antes de acceder por telnet. Si no lo hace, no se permitirá el acceso al modo habilitado y observará un mensaje de error y se le desconectará. Además cuando no exista una contraseña del modo habilitado e intentemos conectarnos al ruteador mediante Telnet, se recibirá el mensaje **No password set** y el indicador volverá al modo usuario.

4.1.3. Añadir líneas de VTY

Supongamos que nos parece que cinco sesiones de telnet no son adecuadas para nuestra empresa. Quizás por razones de seguridad no deseamos que le resulte sencillo a un atacante el bloquear las cinco líneas de VTY. Sin embargo, existe una mantera de crear más líneas VTY. Después de todo, algunos atacantes podrían asumir que, una vez que han bloqueado lo que piensan que son todas las líneas VTY, han terminado su trabajo y que pueden cambiar de objetivos. Para crear más líneas de VTY, basta con introducir algunos comandos **line vty** con números mayores que 4.

4.1.4. Puerto auxiliar

Si se desea acceder al ruteador de manera remota a través de un módem, tendrá que realizar los mismos pasos. Para establecer la contraseña auxiliar, basta con introducir los siguientes comandos

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line aux 0
Router(config-line)#login
Router(config-line)#password DiFIcilDEaDIviNArAuX
```

No hay que olvidar que las configuraciones del ruteador no exigen de forma predeterminada contraseñas en las líneas auxiliares o de consola. Si se desea exigir las contraseñas en estas líneas, no sólo tiene que establecer una contraseña para ellas, sino también debe configurar un comando login para ellas. Sin el comando login no aparecerá la petición de contraseña y se ignorará la contraseña.

4.1.5. Puerto Telnet

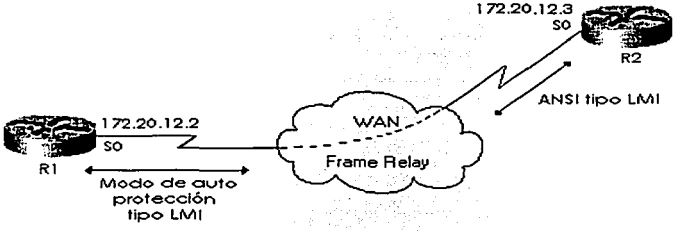
Telnet es simplemente un protocolo de conexión que permite que un usuario de un host establezca una conexión con un host remoto e interactúe como si el usuario estuviera físicamente presente en su terminal. El problema desde el punto de vista de la seguridad es que el tráfico no está cifrado y cuando nos conectamos, tanto el nombre de usuario como la contraseña pueden ser leídos por cualquier dispositivo que esté escuchando en la red.

4.2. Configuración sencilla de Frame Relay

En su forma más simple, Frame Relay proporciona un solo circuito desde una ubicación a otra utilizando una red pública Frame Relay. La figura muestra una configuración sencilla. Los ruteadores Cisco conectados por Frame Relay, se conectan a través de comunicaciones por línea síncrona con un conmutador de Frame Relay. El proveedor de Frame Relay configura un circuito virtual permanente (PVC) a través de la red pública de Frame Relay que conecta a los dos ruteadores. Para configurar correctamente los ruteadores, el proveedor de servicios de la red de Frame Relay

que conecta los dos ruteadores. Para configurar correctamente los ruteadores, el proveedor de la red Frame Relay le debe proporcionar al administrador del ruteador cierta información.
Lo primero y lo más importante, es el tipo de gestión local (LMI) utilizado por el conmutador Frame Relay que se conecta. Las actualizaciones de LMI que pasa el conmutador al ruteador Cisco, actualizarán dinámicamente el ruteador respecto al identificador de conexión del enlace de datos (DLCI - Data Link Connection Identifier) que se utiliza para la conexión del PVC local.

Configuración sencilla de Frame Relay



El sistema operativo IOS de Cisco se aprovecha de la función de ARP inverso del conmutador Frame Relay para determinar la dirección IP remota del ruteador del extremo lejano del PVC. La utilización de ARP inverso le permite el IOS de Cisco asignar automáticamente el DLCI local a la dirección IP remota asociada.

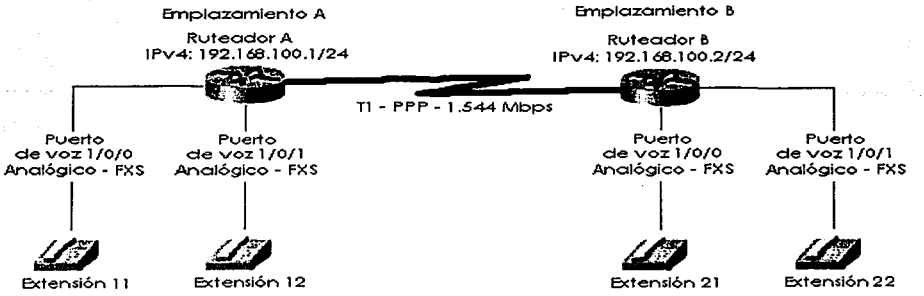
4.2.1. Red sencilla de voz sobre IP

A continuación se presentará la configuración de los dos ruteadores que conforman la red.

- Cada emplazamiento tiene un ruteador Cisco 2610, que se utiliza para tener conectividad entre emplazamientos a través de un enlace T1 y para enlazar dos teléfonos analógicos en cada emplazamiento. En cada ruteador 2600 está instalado un NM-2V con una VIC-2FXS, lo que proporciona conectividad para dos teléfonos analógicos y deja sitio para una VIC adicional de dos puertos que se puede añadir posteriormente.

4.2.2. Resumen de la red

- Ruteadores:
  - Emplazamiento A: 2610-(1) NM-2V con VIC-2FXS; (1) WIC-2T
  - Emplazamiento B: 2610-(1) NM-2V con VIC-2FXS; (1) WIC-2T
- Protocolos: IP con enrutamiento estático.
- Enlaces WAN: Del emplazamiento A al emplazamiento B –T1 dedicado de punto a punto.
- Estaciones de gestión:
  - SNMP: ninguna.
  - Syslog: Ninguna.
- Plan de QoS: precedencia de IP mediante la puesta en cola ecuánime ponderada (WFQ). El T1 proporciona un amplio ancho de banda que admite un máximo de dos llamadas concurrentes entre los emplazamientos. La asignación de un valor de precedencia de IP igual a 5 asegura que el planificador de la WFQ dará prioridad automáticamente al tráfico de voz.



Configuraciones Básicas:

La configuración básica para el emplazamiento A es la siguiente:

```
Emplazamiento A- configuración del ruteador.
!
version 12.0
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service top-small-servers
!
hostname SiteA2610
!
logging buffered 16384 debugging
enable password xxxx
!
ip subnet-zero
no ip domain-lookup
ip host siteB2600 192.168.100.2
ip host SB 192.168.100.2
!
voice-port 1/0/0
  description conexión al teléfono 1 del emplazamiento A
!
voice port 1/0/1
  description conexión al teléfono 2 del emplazamiento A
!
dial-peer voice 1 pots
  destination pattern 11
  port 1/0/0
!
dial-peer voice 2 pots
  destination pattern 12
  port 1/0/1
!
dial-peer voice 3 voip
  destination pattern 2
  ip precedence 5
  no vad
```

```
  session target ipv4:192.168.100.2
!
interface Ethernet0/0
  description conexión al puerto 1/0 de LAN - SW
  ip ardes 192.168.1.1 255.255.255.0
  no ip directed-broadcast
!
interface serial0/0
  description ID de circuito de T1 con Emplazamiento B:11104040
  ip address 192.168.100.1 255.255.255.0
  no ip directed-broadcast
  encapsulation ppp
  no ip mroute-cache
!
interface serial 0/1
  description S0/1: no utilizado
  no ip address
  no ip-directed-broadcast
  shutdown
!
ip classless
ip route 192.168.2.0 255.2553.255.0 192.168.100.2
no ip http server
!
line con 0
  password 7 060506324F41
  login
  modem Dialin
  flowcontrol hardware
line vty 0 4
  password 7 060506324F41
  login
!
no scheduler allocate
end
```

La configuración básica para el Emplazamiento B es la siguiente:

```
Emplazamiento B- configuración del router.
!
version 12.0
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service top-small-servers
!
hostname SiteB2610
!
logging buffered 16384 debugging
enable password xxxx
!
ip subnet-zero
no ip domain-lookup
ip host SiteA2600 192.168.100.1
ip host SA 192.168.100.1
!
voice-port 1/0/0
  description conexión al teléfono 1 del emplazamiento B
!
voice port 1/0/1
  description conexión al teléfono 2 del emplazamiento B
!
```

```
dial-peer voice 1 pots
  destination pattern 21
  port 1/0/0
!
dial-peer voice 2 pots
  destination pattern 22
  port 1/0/1
!
dial-peer voice 3 voip
  destination pattern 1
  ip precedence 5
  no vad
  session target ipv4:192.168.100.1
 !
interface Ethernet0/0
  description conexión al puerto 1/1 de LAN - SWB
  ip ardes 192.168.2.1 255.255.255.0
  no ip directed-broadcast
!
interface serial0/0
  description ID de circuito de T1 con Emplazamiento A:11104040
  ip address 192.168.100.2 255.255.255.0
  no ip directed-broadcast
  encapsulation ppp
  no ip mroute-cache
!
interface serial 0/1
  description S0/1: no utilizado
  no ip address
  no ip-directed-broadcast
  shutdown
!
ip classless
ip route 192.168.1.0 255.2553.255.0 192.168.100.1
no ip http server
!
line con 0
  password 7 104D000A0618
  transport input none
line aux 0
  password 7  060506324F41
  login
  modem Dialin
  flowcontrol hardware
line vty 0 4
  password 7 060506324F41
  login
!
no scheduler allocate
end
```

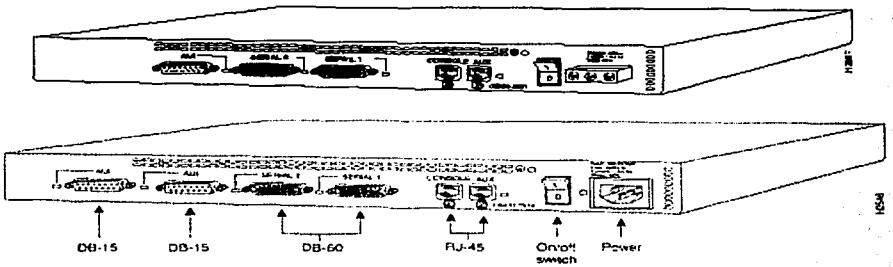
4.2.3. Revisión de la configuración

Las definiciones del Puerto de voz y Puerto de marcación son la base de la conectividad de voz. Los puertos de voz simplemente identifican el dispositivo al que están conectados. Los vecinos o semejantes de marcación 1 y 2 asignan números telefónicos a los puertos de voz físicos. El vecino de marcación 3 define la llamada de VoIP con el emplazamiento B. los bits de precedencia de IP se establecen a 5, lo que proporciona prioridad a la llamada de voz en el planificador de la puesta en cola ecuánime ponderada que se ejecuta en el puerto serie. Además debido al abundante ancho

de banda, la detección de la actividad de voz está inhabilitada. El comando Clases de IP que el ruteador reenvíe los datagramas IP en función de de superredes. La única ruta IP es para la red del emplazamiento B (192.168.2.0/24). En este escenario sencillo no se necesita un protocolo de enrutamiento IP.

4.3. Ruteador serie 2500 de Cisco

Los ruteadores Cisco 2500 vienen con la tecnología EPROM flash para simplificar el mantenimiento de software. Estos sistemas soportan una variedad de juegos característicos de software del sistema operativo, para que se pueda escoger un juego característico que soporte un ambiente protocolar específico.



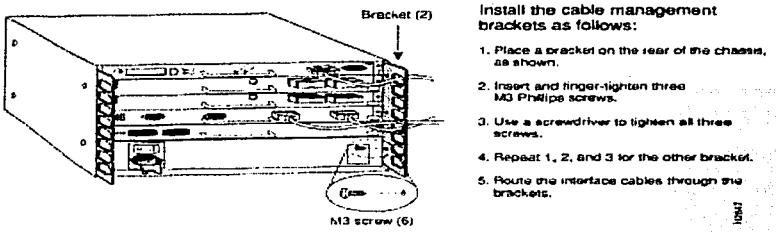
Algunos modelos con una misión específica, contienen menos memoria y menos funcionalidad de hardware para soportar un subconjunto de protocolos. Cada modelo con una misión específica puede ser actualizado para una capacidad completa de ruteador instalando un juego nuevo característico de software del sistema operativo de Cisco, y si fuera necesario, se podría agregar más memoria

Los modelos de la serie 2500 de Cisco pueden ser divididos en las siguientes categorías:

- Ruteadores LAN sencillos modelos 2501, 2502, 2503, 2504, 2520, 2521, 2522 y 2523
- Ruteadores de nivel de entrada de misión específica, modelos 2501CF, 2501LF, 2502CF, 2502LF, 2503I, 2504I, 2520CF, 2520LF, 2521CF, 2521LF, 2522CF, 2522LF, 2523CF y 2523LF
- Combinaciones de Router/hub modelos 2505, 2507 y 2516,
- Servidores de acceso modelos 2509 a 2512
- Ruteadores LAN duales, modelos 2513, 2514 y 2515
- Ruteadores Modulares modelos 2524 y 2525 (Opcional DSU/CSU integrado o NT-1)

La serie 7500 de Cisco incluye los siguientes ruteadores: 7505, 7507,7513, y 7576. La serie de ruteadores de Cisco 7500 soportan multiprotocolo, ruteo multimedia y puenteo con una amplia variedad de protocolos y cualquier combinación de ATM, BRI, canal conectado, E1, T1, y T3, medios canalizados Ethernet, Fast Ethernet, FDDI, (HSSI),
multicanal, PRI, Paquete sobre OC-3, seriales síncronas, y Token Ring.

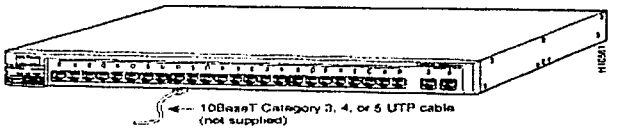
Ruteador 7505 de Cisco



4.4. Switches

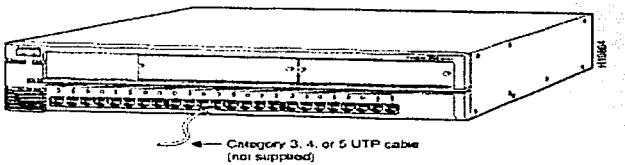
Los switches Catalyst 1900 proporcionan hasta 24 conexiones Ethernet Switcheadas de 10 Mbps para los dispositivos compatibles con 10BaseT (tales como las estaciones de trabajo sencillas y hubs 10BaseT) y una conexión 10 Mbps hacia un AUI. Los switches también proporcionan dos conexiones 100BaseT hacia los servidores y troncales.

Ruteador 2514 de Cisco



Los switches Ethernet de la serie 2820 proporcionan 25 conexiones Ethernet Switcheadas de 10 Mbps: 24 conexiones de 10 Mbps hacia dispositivos compatibles con 10BaseT (tales como las estaciones de trabajo sencillas y hubs 10BaseT) y una conexión de 10 Mbps hacia un AUI. Los switches con los módulos opcionales Catalyst 2820 instalados pueden proporcionar 100BaseT, FDDI, y conectividad ATM hacia servidores y troncales.

Switch Catalyst 2820 de Cisco



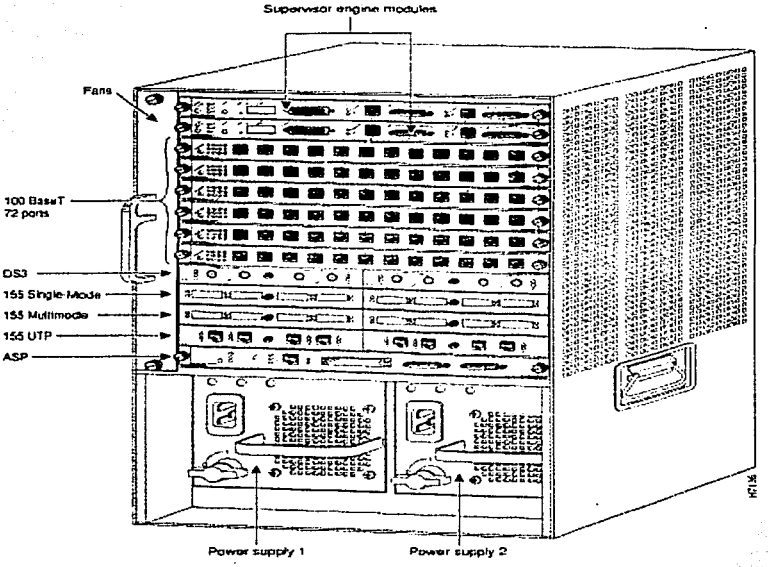
El switch Catalyst 5500 proporciona Ethernet y Fast Ethernet switcheado de alta densidad, Token Ring y ATM para ambos cableados y aplicaciones de central de datos, usando UTP multimodo y cable de fibra óptica mono modo. El switch Catalyst 5500 soporta conexiones switcheadas Ethernet de 10 Mbps, conexiones repetidoras Ethernet, y Fast Ethernet Switcheado de 100 Mbps con conexiones troncales hacia Fast Ethernet, ATM, FDDI, y CDDI. Típicamente, las interfases Ethernet del

Catalyst 5500 conectan puestos de trabajo y repetidores mientras las interfaces Fast Ethernet se conectan a las estaciones de trabajo, servidores, interruptores, y ruteadores.

4.4.1. Descripción del sistema

El chasis del switch Catalyst 5500 tiene 13 ranuras. La ranura 1, la cual está dedicada al módulo del artefacto supervisor II, proporciona switcheo, manejo local y remoto, e interfaces Fast Ethernet duales. La ranura 2 contiene un artefacto supervisor redundante adicional II como respaldo en caso de que el primer módulo falle. Una falla del artefacto supervisor activo II es detectado por el módulo de espera que toma el mando de las funciones de switcheo del artefacto supervisor II.

Switch 5500 de Cisco



Las ranuras restantes están disponibles para cualquier combinación de Ethernet, Fast Ethernet, FDDI/CDDI, y ATM. Si no se requiere un artefacto supervisor redundante II, la ranura 2 está disponible para cualquier módulo. El Catalyst 5500 acepta módulos LightStream 1010 ATM en el chasis, en las ranuras 9 hasta la 13. La ranura 13 es una ranura especializada que acepta sólo módulo del procesador del switch ATM.

4.5. Configuración Frame Relay real de un ruteador

La siguiente es la configuración de un ruteador de una concesionaria General Motors, la cual opto por configurar su ruteador con encapsulamiento Frame Relay.
Al principio de la configuración se puede apreciar el comando **show running-configuration** que es el que despliega toda la información. También se ve la versión del sistema operativo, el nombre del ruteador y un aspecto muy importante que también muestra este comando en la contraseña.
Las interfases que se muestran revelan sus datos de configuración, como lo son su dirección IP y su máscara, con la cual podemos deducir los bits de la subred.
Para las interfases seriales, el encapsulamiento es Frame Relay, se muestra su DLCI y el tipo de LMI que en este caso es ANSI.
Más abajo se aprecia la configuración de la contraseña de los puertos VTY, y por último por medio del comando show versión se muestran los detalles referentes al sistema operativo, modelo de ruteador y la localidad de memoria y su configuración en la cual se encuentra guardada la imagen del sistema operativo

```
□□□□□□□□□          □□□□□□□□□
GM_IZTACALCO_MOTORS#sh run
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname GM_IZTACALCO_MOTORS
!
enable password prov
!
memory-size iomem 20
ip subnet-zero
!
!
!
interface Ethernet0/0
 ip address 172.27.130.1 255.255.255.128
 no ip directed-broadcast
!
 interface Serial0/0
 ip address 172.27.253.169 255.255.254.0
 no ip directed-broadcast
 encapsulation frame-relay
 no ip mroute-cache
 frame-relay interface-dlci 191
 frame-relay lmi-type ansi
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.27.253.1
no ip http server
!
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password prov
 login
!
no scheduler allocate
```

```
end

GM_IZTACALCO_MOTORS#    sh ver
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IS-M), Version 12.0(3)T3,  RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Thu 15-Apr-99 16:12 by kpma
Image text-base: 0x80008088, data-base: 0x80A05BAC

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

GM_IZTACALCO_MOTORS uptime is 43 minutes
System restarted by power-on
System image file is "flash:c2600-is-mz.120-3.T3"

cisco 2610 (MPC860) processor (revision 0x300) with 26624K/6144K bytes of memory.
Processor board ID JAD06080CMW (3516280498)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102

GM_IZTACALCO_MOTORS# sh hard
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IS-M), Version 12.0(3)T3,  RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Thu 15-Apr-99 16:12 by kpma
Image text-base: 0x80008088, data-base: 0x80A05BAC

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

GM_IZTACALCO_MOTORS uptime is 44 minutes
System restarted by power-on
System image file is "flash:c2600-is-mz.120-3.T3"

cisco 2610 (MPC860) processor (revision 0x300) with 26624K/6144K bytes of memory.
Processor board ID JAD06080CMW (3516280498)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

4.6. Configuración de voz sobre Frame Relay

En esta configuración la cual se trata de un ruteador de una franquicia BMW en la ciudad de Toluca. Este ruteador fue configurado con la característica de que admite el encapsulamiento Frame Relay para voz y para datos simultáneamente.
Puede apreciarse que el ruteador tiene una interfase Fast Ethernet configurada con una subred, la cual seguramente está conectada a un switch.

En la interfase serial, se puede ver la descripción "Enlace Hacia Santiago Tianguistenco" su DLCI y además la referencia de que se trata de un enlace de voz sobre Frame Relay "vofr cisco".
Mas abajo se precia el ruteo y sus redes que se están anunciando hacia los demás ruteadores
En esta sección se muestra el CIR y el ancho de banda que se estableció para este enlace de voz, el cual es de 24000 seguido por la configuración de los puertos de voz y su extensión que se debe marcar. Por ultimo de muestra un informe generado por el comando Show versión y show hardware.

```
sh run
Building configuration...

Current configuration : 1320 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Star_Haus-Toluca
!
enable password prov
!
memory-size iomem 15
ip subnet-zero
!
!
!
interface FastEthernet0/0
 ip address 172.16.11.1 255.255.255.248
 speed auto
!
interface Serial1/0
 no ip address
 encapsulation frame-relay
 frame-relay traffic-shaping
 frame-relay lmi-type ansi
!
interface Serial1/0.1 point-to-point
 description Enlace a Santiago Tianguistenco
 ip address 192.168.254.38 255.255.255.252
 frame-relay interface-dlci 250
  class FR
  vofr cisco
!
router eigrp 10
 network 172.16.0.0
 network 192.168.254.0
 no auto-summary
 no eigrp log-neighbor-changes
!
ip classless
no ip http server
ip pim bidir-enable
!
!
!
map-class frame-relay FR
 frame-relay cir 48000
 frame-relay bc 1000
 no frame-relay adaptive-shaping
 frame-relay fair-queue
 frame-relay voice bandwidth 24000
 frame-relay fragment 80
```

```
!
call rsvp-sync
!
voice-port 0/0
!
voice-port 0/1
!
dial-peer cor custom
!
!
!
dial-peer voice 1 pots
 destination-pattern 8010
 port 0/0
!
dial-peer voice 2 pots
 destination-pattern 8010
 port 0/1
!
dial-peer voice 100 vofr
 destination-pattern ....
 session target Serial1/0 250
 no vad
!
!
line con 0
line aux 0
line vty 0 4
 password prov
 login
!
end

Star_Haus-Toluca#sh ver
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-SV3Y-M), Version 12.2(4)XW, EARLY DEPLOYMENT
RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 14-Nov-01 01:18 by ealyon
Image text-base: 0x80008124, data-base: 0x80CA8C08

ROM: System Bootstrap, Version 12.2(1r)XE1, RELEASE SOFTWARE (fc1)
ROM: C1700 Software (C1700-SV3Y-M), Version 12.2(4)XW, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)

Star_Haus-Toluca uptime is 2 days, 21 hours, 51 minutes
System returned to ROM by power-on
System image file is "flash:c1700-sv3y-mz.122-4.XW.bin"

cisco 1751 (MPC860P) processor (revision 0x200) with 55706K/9830K bytes of
memory.
Processor board ID JAD0611076H (2608522590), with hardware revision 0000
MPC860P processor: part number 5, mask 2
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
1 Serial(sync/async) network interface(s)
2 Voice FXS interface(s)
32K bytes of non-volatile configuration memory.
32768K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

```
Star_Haus-Toluca#sh hard
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-SV3Y-M), Version 12.2(4)XW, EARLY DEPLOYMENT
RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 14-Nov-01 01:18 by ealyon
Image text-base: 0x80008124, data-base: 0x80CA8C08

ROM: System Bootstrap, Version 12.2(1r)XE1, RELEASE SOFTWARE (fc1)
ROM: C1700 Software (C1700-SV3Y-M), Version 12.2(4)XW, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)

Star_Haus-Toluca uptime is 2 days, 21 hours, 51 minutes
System returned to ROM by power-on
System image file is "flash:c1700-sv3y-mz.122-4.XW.bin"

cisco 1751 (MPC860P) processor (revision 0x200) with 55706K/9830K bytes of
memory.
Processor board ID JAD0611076H (2608522590), with hardware revision 0000
MPC860P processor: part number 5, mask 2
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
1 Serial(sync/async) network interface(s)
2 Voice FXS interface(s)
32K bytes of non-volatile configuration memory.
32768K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102

Star_Haus-Toluca#sh□ □□ □□
```

Como se puede apreciar, estas configuraciones poseen el password y sus detalles de configuración muy bien mostrados, con las cuales podríamos hacer cambios en la configuración del ruteador

Recientemente se ha venido usando una opción de los ruteadores que integra la voz sobre encapsulamiento Frame Relay, el cual implica una ventaja, si se tiene una red, usar esas tramas para transmitir voz, con lo que se ahorran recursos en gran medida. Este avance se puede lograr gracias a las técnicas de compresión de la voz, a tal grado de mantener la calidad del audio como si se tratara de 64 Kbps.

Capítulo 5 Prácticas

Introducción

Este último capítulo contiene las prácticas que se desarrollarán en el laboratorio, con ayuda del simulador, como ya se mencionó con anterioridad. También una explicación de cómo se el instructor debe prepararse para impartir las prácticas en el laboratorio.

5.1. Estructura de las prácticas

Para llevar a cabo los temas que se plantearon a lo largo de los capítulos anteriores se llevaron a cabo 8 prácticas, las cuales van desde la explicación del sistema operativo hasta el desarrollo de una red Frame Relay, con el objetivo de hacer que el alumno desarrolle un interés hacia la configuración de los dispositivos de interconexión de redes, por medio del aprendizaje del sistema operativo, a través del simulador. Cada una de las prácticas consta de cuatro partes, las cuales son:

- Cuestionario preliminar
- Introducción
- Desarrollo de la práctica
- Cuestionario

El cuestionario preliminar esta hecho para que el alumno investigue cierta información y se involucre con los conceptos que se requieren para realizar la práctica

La introducción muestra un resumen de lo que va a ser tratado en la práctica, y contiene información de datos técnicos y teóricos.

El desarrollo de la práctica es el trabajo a realizar en el laboratorio con ayuda del instructor. También cuenta con explicaciones gráficas de los pasos a seguir, además de tablas con información y tablas para que se escriba la información que se realizó en la elaboración de la práctica.

El cuestionario tiene el propósito de reafirmar el trabajo en el laboratorio, con preguntas que en algunos casos solo se pondrán resolver practicando las configuraciones y también con información que se obtuvo en la elaboración de la práctica.

5.1.1. Contenido de las prácticas

El orden con que se plantea la elaboración de las prácticas tiene como objetivo introducir al alumno en la configuración de los ruteadores desde el punto de vista del campo laboral, en otras palabras, los que se pretende es darle al alumno cierta información técnica, la cual no está prevista en los cursos normales.

Práctica 1 Esta práctica es una introducción del sistema operativo de Cisco, el modelo OSI y otros conceptos necesarios para comprender como se lleva a cabo el intercambio de datos. Se plantean las bases para lo que se desarrollará en las prácticas siguientes.

Práctica 2 Es la exploración inicial del simulador, sus herramientas y el reconocimiento del ruteador, sus interfases y una breve mirada a sus características y capacidades. Se hace uso de los comandos de monitoreo y se establece una contraseña para un ruteador.

Práctica 3 El objetivo principal de esta práctica es establecer las bases para el diseño de una red LAN, iniciando con conceptos de redes LAN en la introducción, para después configurar la red con ayuda del simulador. También se involucran conceptos de direccionamiento IP, haciendo que el alumno realice el plan de numeración.

Práctica 4 Gracias al antecedente de la práctica 3, el subnetting y el ruteo son los temas que se cubren en esta práctica, dejando que el alumno elabore la numeración IP de una red y sus respectivas subredes. La red consta de dos subredes LAN unidas por medio de dos ruteadores, con lo cual se logra la conectividad entre todos los dispositivos.

Práctica 5 Las redes LAN virtuales son el tema en esta práctica, ya que tienen la particularidad de aislar grupos de PC's dentro de una red, privilegiando la información y aminorando el costo de la red. Por estos motivos, el alumno demuestra las características y beneficios de este tipo de redes, configurando por completo la red

Práctica 6 Las prácticas siguientes tratan de redes WAN y sus protocolos, por lo que en la práctica 6 se configura el protocolo punto a punto, que es de gran importancia para la conectividad entre los ruteadores. También se configura dentro de este tipo de enlace, el aspecto de la seguridad, configurando las contraseñas correspondientes.

Práctica 7 En esta práctica se configura por completo los enlaces ISDN, que gracias las características del simulador se pueden tratar los temas correspondientes como por ejemplo, la configuración del marcaje telefónico hacia el proveedor de servicio, entre otras cosas.

Práctica 8 En esta última práctica se trata el tema de Frame Relay, configurando por medio de un enlace entre 4 PC's, para esto se configuran sobre una interfase serial de cada ruteador, varias subinterfases, con su respectiva dirección IP y su máscara.

5.2. Prácticas para el laboratorio de comunicaciones

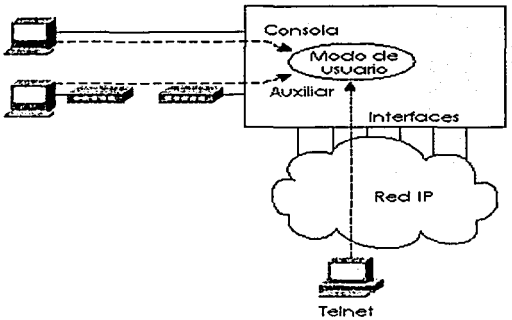
Para desarrollar las prácticas, el instructor debe documentarse sobre el tema por medio de los capítulos anteriores de esta tesis, ya que cuentan con la información complementaria de lo que se tiene que tratar cada una de las prácticas.
El instructor que lo desee puede ahondar en los temas que se crea necesario, diseñando configuraciones de red o aportando información mas reciente de los temas que se tratan, ya que el simulador lo permite gracias a sus herramientas con las que cuenta.
A continuación se presentan los formatos de las prácticas.

Práctica 1 Sistema Operativo de Cisco

Introducción:

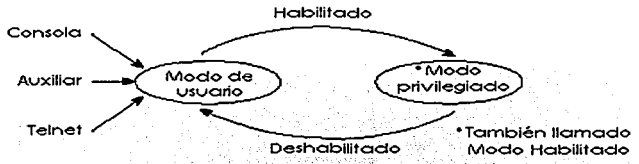
En la industria una de los principales fabricantes de ruteadores a nivel mundial es Cisco, por lo que se estudiará el sistema operativo que esta incorporado en los ruteadores de este fabricante.
IOS es el nombre del sistema operativo que se encuentra en la mayoría de los ruteadores de Cisco, dentro de los cuales corre el sistema operativo con su línea de comandos de la interfase (CLI – Command Line Interface). Estos comandos son de gran importancia, ya que se usan para hacer las configuraciones en los ruteadores. Para usar los comandos, se tiene que acceder por una de las tres opciones de conexión

Acceso al ruteador



Una vez ingresando al ruteador por medio de una de las tres opciones que son Consola, Auxiliar y Telnet se requiere de una contraseña para que se pueda hacer uso de dos opciones de configuración, las cuales son el modo usuario y el modo privilegiado, estos modos nos permiten solo ver la configuración, o hacer cambios en el ruteador respectivamente.

Modos de usuario y privilegiado



Comandos de ayuda

Tecleando	La ayuda que se obtiene
?	Ayuda para todos los comandos disponibles en este modo
Help	Texto que describe cómo conseguir la ayuda, no se da ayuda del comando
Command ?	Texto de ayuda que describe todas las primeras opciones del parámetro para el comando.
Com?	Una lista de comandos que comienzan con "com"
Command parm?	Este tipo de ayuda están todos los parámetros comenzando con "parm". Nótese que no hay espacio entre "parm" y "?"
Command parm<Tab>	Si el usuario aprieta la tecla Tab, el CLI deletreará el resto de este parámetro a la línea del comando para el usuario, o no hará nada. Si el CLI no hace nada, significa que esta serie de caracteres representa más de un posible parámetro siguiente, así que el CLI no sabe qué comando deletrear
Command parm1 ?	Si un espacio se inserta antes del signo de interrogación, el CLI lista todos los próximos parámetros y da una explicación breve de cada uno

El Cisco Discovery Protocol (CDP) se usa por los ruteadores y switches de Cisco para determinar la información básica sobre los ruteadores vecinos. Se puede usar esta información para aprender las direcciones de otros dispositivos cuando no se tienen las contraseñas para ingresar en otro dispositivo. Cualquier ruteador de Cisco con interfases LAN, HDLC, Frame Relay, y ATM soporta el protocolo CDP.

- El modelo OSI

OSI es el modelo de referencia del Sistema de Interconexión Abierto para las comunicaciones. Las capas superiores del modelo OSI (aplicación, presentación, y sesión, capas 7, 6, y 5) se orientan más hacia los servicios de las aplicaciones. Las cuatro capas más bajas (transporte, red, enlace de datos, y física, capas 4, 3, 2, y 1) se orientan más hacia el flujo de datos de extremo a extremo a través de la red. Se trabajará principalmente con los problemas en las capas más bajas, en particular con la Capa 2 en donde se lleva a cabo la conmutación, y la Capa 3, donde el ruteo se lleva a cabo

Pueden ganarse muchos beneficios del proceso de separar las funciones o tareas de conectar una red de en pedazos más pequeños o capas, y definir las interfases estandarizadas entre estas capas. Un beneficio obvio es que los protocolos individuales o capas son menos complejas y por consiguiente pueden definirse con gran detalle.
Una capa usa los servicios de la capa inmediatamente debajo de ella. Por consiguiente, es más fácil recordar lo que cada capa hace.

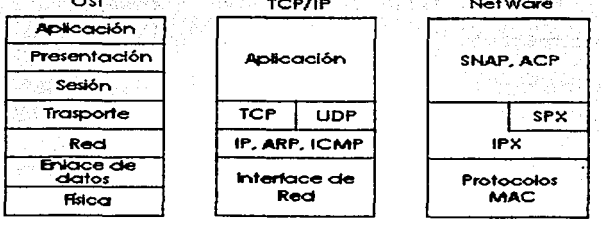
Nombre de la Capa OSI	Descripción Funcional	Ejemplos
Aplicación (Capa 7)	Interfase de Usuario	Telnet, HTTP
Presentación (Capa 6)	Cómo los datos son presentados Proceso especial, como la encriptación	JPEG, ASCII, EBCDIC
Sesión (Capa 5)	Los mantiene los datos separados de las diferentes aplicaciones	Los sistemas operativos y planificación de acceso de aplicación
Transporte (Capa 4)	Entrega Multiplexada fiable o no fiable	TCP, UDP, SPX
Red (Capa 3)	Direccionamiento lógico, el cual los ruteadores usan para la Determinación del camino	IP, IPX
Enlace de Datos (Capa 2)	La combinación de bits en bytes, y bytes en Tramas Acceso al medio usando direcciones MAC detección de error y recuperación del error	802.3/802.2, HDLC
Física (Capa 1)	Movimiento de los bits entre los dispositivos Especificación de voltaje, velocidad del alambre, y pines de salida del cable	EIA/TIA-232, V.35

- Encapsulamiento de datos

El concepto de poner los datos detrás de las cabeceras (y antes de las banderas) para cada capa, se llama típicamente Encapsulamiento. Cuando cada capa crea su cabecera, pone los datos en ella por la siguiente capa mas alta detrás de su propia cabecera, encapsulando los datos de la capa más alta. En el caso de un protocolo de enlace de datos (Capa 2), la cabecera y los datos de la capa 3 son puestos entre la cabecera de la capa 2 y la bandera de la capa 2. La capa física no usa encapsulamiento porque no usa cabeceras o banderas.

- Los protocolos TCP/IP y NetWare

Protocolos OSI, TCP/IP y NetWare



Como se ilustra en la figura, los protocolos IP e IPX tienen una semejanza más cercana con la capa de red de OSI. Claramente, IP está en la capa 2 de TCP/IP, pero para el uso consistente de terminología, se llama normalmente protocolo de Capa 3 porque sus funciones se asemejan estrechamente con la capa 3 de OSI. IP e IPX definen el direccionamiento lógico, ruteo, el aprendizaje la información de, ruteo y las reglas de la entrega de extremo a extremo.
Como con las Capas 1 y 2 de OSI (física y enlace de datos, respectivamente), las más bajas capas de cada pila simplemente se refieren a otras especificaciones muy conocidas.

- Funciones de la capa de Transporte de OSI

La capa de transporte define varias funciones. Dos características importantes, son recuperación de error y control de flujo. La capa de transporte puede proveer la retransmisión (recuperación de error) y puede ayudar a evitar la congestión (control de flujo). Los protocolos de la capa de transporte se categorizan típicamente como orientado a conexión o no orientado a conexión.

- Protocolos orientados a conexión Contra los no orientados a Conexión

Protocolo orientado a conexión: Es un protocolo cualquiera que requiere un intercambio de mensajes antes de que el traslado de los datos empiece o tiene una correlación preestablecida requerida entre dos puntos finales.
Protocolo no orientado a Conexión: Es un protocolo que no requiere un intercambio de Mensajes y no requiere una correlación preestablecida entre dos puntos finales como el correo electrónico.
El control de flujo es el proceso de controlar la tasa a la que una computadora envía los datos. Dependiendo del protocolo en particular, ambos el remitente y el receptor de datos (así como cualquier ruteador, puentes, o interruptores intermedios) podría participar en el proceso de controlar el flujo del remitente al receptor.

• Funciones de la capa de red de OSI

Las dos funciones claves para cualquier Protocolo de Capa 3 son el ruteo y el direccionamiento. Estas dos funciones se entrelazan y se entienden mejor considerando los dos al mismo tiempo.

• Ruteo

El ruteo puede pensarse como un proceso de tres pasos, como se muestra en la Figura.

Los tres pasos del ruteo

Paso 1 Enviando los datos de la computadora fuente hacia algún ruteador cercano
Paso 2 Entregando los datos de un ruteador cerca de la fuente a un ruteador cerca del destino
Paso 3 Entregando los datos del ruteador cerca del destino a la computadora de

- Direccionamiento en la Capa de Red (Capa 3)

Las direcciones de la capa de red son agrupaciones basadas en la locación física en una red. Las reglas difieren para algunos protocolos de la capa de red, pero el concepto de la agrupación es idéntico para IP, IPX, y AppleTalk. En cada uno de éstos los protocolos de la capa de red, no pueden separarse todos los dispositivos con las direcciones en el mismo grupo, no pueden ser separadas de cada uno de los otros por un ruteador que se configure para dirigir ese protocolo, respectivamente. Dicho de otra manera, todos los dispositivos en el mismo grupo (subred/red/rango de cable) deben conectarse al mismo enlace de datos; por ejemplo, todos los dispositivos deben conectarse al mismo Ethernet.

El ruteo confía en el hecho de que las direcciones de la capa 3 son agrupadas juntas. Las tablas de ruteo para cada protocolo de la capa de red pueden referirse al grupo, no a cada dirección individual.

La mayoría de los esquemas de direccionamiento de la capa de red (Capa 3), se crearon con las metas siguientes:

- El espacio de dirección debe ser bastante grande para acomodar la más grande red para la cual los diseñadores imaginaron que el protocolo se usaría.
- Las direcciones deben permitir la asignación única para que la oportunidad de duplicación de direcciones sea pequeña o no exista
- La estructura de las direcciones debe tener alguna agrupación implicada que se considere que muchas direcciones estén en el mismo grupo.
- En algunos casos se desea, la asignación de direcciones dinámicas.

- Protocolos de ruteo

Los protocolos de ruteo definen la estructura y procedimientos del mensaje, como cualquier otro protocolo. Con los protocolos de ruteo, sin embargo, la meta es no ayudar con la entrega de datos del usuario final, la meta es llenar la tabla de ruteo con todos los grupos destino conocidos y con la mejor ruta para alcanzar cada grupo.

Cuestionario:

¿Cómo se usan los comandos de ayuda? Establecer un ejemplo

¿En que capas de modelo OSI operan los Hubs, Puentes, Switches y Ruteadores? Explique

¿De una explicación de los tres métodos de acceso a un ruteador?

¿Qué es el modo privilegiado?

¿Qué instituciones en México cuentan con un convenio con Cisco Systems?

Cuestionario previo de la Práctica 1

Para la realización de la práctica 1, se requiere resolver las siguientes preguntas relacionadas con el tema de la primera práctica

Investigar acerca de la certificación CCNA de Cisco

¿Que es un ruteador y que funciones cumple?

¿En que capas del modelo OSI opera el ruteador y por que?

Principales arquitecturas de protocolos

Origen del modelo OSI

¿Que función desempeña cada una de las siete capas del modelo OSI?

¿Que capas del modelo OSI, según sus funciones intervienen en el proceso de transmisión de la información a través de la red y explique?

¿Qué es protocolo orientado a conexión y protocolo no orientado a conexión?

Investigar cuales son las principales marcas de distribuidores de ruteadores

Práctica 2 Introducción al simulador

- Simulador

En esta práctica se comenzará la iniciación y exploración del sistema operativo con la ayuda de una herramienta muy importante la cual imita el comportamiento del ruteador en lo referente a su configuración. El simulador nos permite practicar la navegación del sistema operativo y sus comandos, sin contar con el equipo físicamente.

El simulador que se usará será el Boson Router Simulator. Este simulador es el más completo que existe y permite la configuración básica de una red LAN, hasta el desarrollo de una red compleja involucrando enlaces punto a punto, la posibilidad de configurar redes Frame Relay, ISDN y Redes LAN virtuales, etc.
La ventaja que se tiene es obvia, se puede practicar cuando se desee sin el riesgo de dañar el ruteador o hacer mal uso de los enlaces, sin mencionar el costo.

En el simulador se puede elegir de varios modelos de ruteadores, los cuales tienen un número de interfases específico, que va desde una interfase serial y una interfase Ethernet, hasta configuraciones de 10 interfases seriales una Ethernet y una ISDN.

El simulador requiere de un sistema Pentium con 233 Mhz, memoria RAM de 32 Mb, 16 Mb de espacio libre en disco duro y sistema operativo Windows 95/98 SE/2000 ME/ XP.

Objetivo:

El alumno conocerá los dos modos de configuración de usuario y privilegiado, en los cuales se mostrará el uso de los comandos básicos para mostrar un panorama del potencial que se tiene con esta herramienta.

Desarrollo de la práctica

Iniciar el simulador y con la explicación previa del instructor. Ingresar a uno de los cinco ruteadores de la topología predefinida, y obtener los comandos que están disponibles en ese modo, de los comandos que se muestran.

Al iniciar la sesión con un ruteador se debe presionar la tecla Enter, para que en la pantalla se muestre el indicador. El símbolo > significa que se esta en el modo usuario.
Cuando se desea ingresar al modo privilegiado, solo se teclea el comando **enable** y se verá que el indicador cambia de símbolo como se muestra a continuación:

```
Press Enter to Start

Router>
Router>Enable
Router#
```

Estando en este modo, lo siguiente es establecer una contraseña de ingreso al modo privilegiado, para lo que se necesita teclear los comandos **configure terminal:**

```
Router#
Router#configure terminal
Router(config)#
Router(config)#enable password contraseña
Router(config)#exit
Router#exit
Router>
```

Ahora hay que asignar un nombre de identificación al ruteador emitiendo el comando de configuración **hostname**, con lo que se facilitará la configuración cuando existan varios ruteadores involucrados.

- Interfases

Cuando se realicen configuraciones en los ruteadores, es necesario habilitar las interfases con las cuales vamos a trabajar, ya que es importante tener bien identificadas cuales van a ser los enlaces que se van a configurar.
Para ver las interfases con las cuales se cuenta, se usa el comando **show ip interface brief**, estos comandos muestran un breve resumen del estado de las interfases, su protocolo y la dirección IP que se le asigno a cada interfase:

```
Router#show ip interface brief

Interface      IP-Address      OK?  Method  Status                Protocol
Serial0        Unassigned      Yes  Unset   administratively down down
Serial1        Unassigned      Yes  Unset   administratively down down
Ethernet0      Unassigned      Yes  Unset   administratively down down
```

Lo siguiente es habilitar una de las interfases para después ver el resultado, los comandos que se emiten los siguientes:

```
Router#
Router#configure terminal
Router(config)#
Router(config)#interface serial 0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
Router#
```

- Diseño de red

El diseño de red, es una herramienta que nos va a permitir decidir que tipo de red es la que vamos a configurar según nuestros requerimientos, donde se tendrá la oportunidad de elegir los ruteadores switches y conexiones que se deseen.

Para explorar esta herramienta, se debe hacer lo siguiente:

En la barra de herramientas, elegir la opción de diseño de red y plantear una red de dos ruteadores con una un enlace serial entre ellos y una PC conectada a uno de los dos ruteadores por medio de un enlace Ethernet y guardar esa configuración. Iniciar el simulador de nuevo y cargar la topología previamente guardada

Los comandos **show** son de gran importancia cuando se desean ver los detalles de la configuración, estado de las interfases, los protocolos, sub interfases, etc. Estos comandos se pueden ver emitiendo el comando de ayuda **?**

```
Router#sh ?

access-lists
arp                    ARP table
cdp                    CDP information
clock                  Display the system clock
controllers            Interface controller status
flash                  Display information about flash: file system
frame-relay            Frame Relay-information
history                Display the session command history
hosts                  IP domain-name, nameservers, and host table
interfaces             Interface status and configuration
ip                     IP information
ipx                    Novell IPX information
isdn                   ISDN information
ntp                    Network time protocol
protocols              Active network routing protocols
running-config         Current operating configuration
sessions               Information about Telnet connections
startup-config         Contents of startup configuration
terminal               Display terminal configuration parameters
users                  Display information about terminal lines
version                System hardware and software status
```

De todas estas opciones que se tienen para los comandos show, elegir el mas apropiado para ver la configuración actual de las interfases, después de que se han dado de alta.

Por último, usar algunos comandos show y anotar su función en la siguiente tabla:

Comando(s)	Descripción

- Cuestionario

¿Qué modelos de ruteadores se pueden elegir?

¿Por qué hay diferentes tipos de conexiones en el diseñador de red?

¿Por que cuando se habilitaron las interfases aparecía la leyenda down en las interfases seriales y en la Ethernet up?

¿Para que sirve la contraseña que estableció?

¿Cuál es la ruta a seguir cuando se quiere ver las opciones de encapsulamiento que se pueden establecer?

Cuestionario preliminar de la práctica 2

¿Qué es un simulador?

Diga tres ejemplos de simuladores

¿Qué es el modo usuario y el modo privilegiado?

¿Para que sirve la herramienta de diseño de red?

¿De que tipos de interfases se puede contar en este simulador?

¿Cuántas interfases se tienen en el switch 1912 y de que capacidad son?

Práctica 3 Introducción a redes LAN

Objetivo de la práctica:

Al Término de esta práctica el alumno será capaz de:

- Reconocer los comandos básicos para la configuración de los switch de la serie 1900.
- Configurar las interfases del switch para establecer una red LAN
- Completar la red con la conexión hacia un ruteador

Introducción:

Un bús es compartido entre todos los dispositivos en el Ethernet usando un algoritmo para acceder al bús (CSMA/CD). Este algoritmo funciona así: El remitente está listo para enviar una trama. El dispositivo escucha para detectar si cualquier trama está recibiéndose actualmente. Cuando el Ethernet está en silencio, el dispositivo empieza a enviar la trama. Durante este tiempo, el dispositivo transmisor escucha para asegurarse que la trama que está enviando, no choca con una trama que otra estación está enviando. Si no ocurre ninguna colisión, los bits de la trama enviada se reciben de regreso con éxito. Si una colisión ocurre, el dispositivo envía una señal de atasco y entonces espera una cantidad al azar de tiempo antes de repetir el proceso, de nuevo escucha para oír si otra trama está recibiéndose.

Debido al algoritmo CSMA/CD, Ethernet 10Base5 y 10Base2 se volvió más ineficaz bajo mayores cargas de tráfico. De hecho, dos características negativas del algoritmo CSMA/CD son las siguientes:

- Todas las tramas colisionadas enviadas no se reciben correctamente, así que cada estación transmisora debe reenviar las tramas. Esto es un desperdicio de tiempo en el bús y aumenta la latencia para entregar las tramas colisionadas.

- La latencia puede aumentar para las estaciones que esperan que el Ethernet este en silencio antes de enviar sus tramas. Los dispositivos deben esperar antes de enviar una trama si otra trama ya está enviándose por otra estación. Esto aumenta la latencia mientras se espera que la trama entrante se complete.

• Direccionamiento LAN

Una función importante de direcciones MAC es identificar o direccionar las tarjetas de interfase LAN en el Ethernet, Token Ring, y FDDI LANs. Las tramas entre un par de estaciones LAN usan un campo de dirección fuente y destino para identificarse cada uno. Estas direcciones se llaman direcciones unicast o direcciones individuales, debido que ellas identifican una tarjeta individual LAN.

Teniendo una única dirección unicast MAC en todas las tarjetas LAN, es una meta del IEEE, para que la organización administre un programa en cual los fabricantes codifican la dirección MAC en la tarjeta LAN, normalmente en un chip ROM. La primera mitad de la dirección es un código que identifica al vendedor. La segunda parte simplemente es un número único entre tarjetas que el vendedor ha fabricado. A estas direcciones se les llama direcciones quemadas.

- Puenteo transparente

Se le llama transparente porque los dispositivos del punto final no necesitan saber que existe(n) puente(s). En otros términos, las computadoras en la LAN no se comportan diferentes en la presencia o ausencia de puentes transparentes. El puenteo transparente es el proceso de remitir las tramas, cuando sea apropiado.

- Switcheo LAN

La lógica interior del switch se optimiza para realizar la función básica de escoger cuándo remitir y cuándo filtrar una trama. La lógica básica de un LAN switch es la siguiente:

Paso 1	Se recibe una trama
Paso 2	Si el destino es una transmisión o multicast, remitir en todos los puertos.
Paso 3	Si el destino es un unicast y la dirección no está en la tabla de direcciones, remitir en todos los puertos.
Paso 4	Si el destino es un unicast y la dirección está en la tabla de direcciones, remite la trama fuera del puerto asociado, a menos que la dirección MAC este asociada con el puerto entrante.

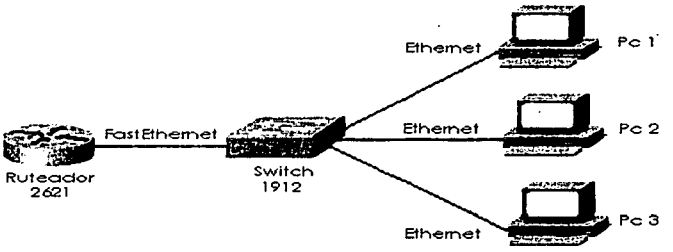
- Configuración predefinida del switch 1900

Los valores predefinidos varían dependiendo de las características del switch. La lista siguiente provee algunas de las especificaciones predefinidas para el switch Catalyst 1900.

- Dirección IP: 0.0.0.0
- CDP: Enabled
- Modo de switcheo: FragmentFree
- Puerto 100BaseT: Auto-negociate duplex mode
- Puerto 10BaseT: Half dúplex
- Árbol de expansión: Enabled
- Contraseña de consola: None

- Desarrollo de la Práctica

Iniciar el simulador t seleccionar en el menú de herramientas la opción de diseño de red. Del cuadro de dispositivos de red, se necesitará un switch modelo 1912, y un ruteador modelo 2621 de la serie 2600, este tipo de ruteador permite la conexión Fast Ethernet, este puerto es indispensable para establecer un enlace troncal de nuestra red LAN.
A continuación seleccionar el tipo de conexiones apropiadas para unir el switch con 3 PC´s, como se muestra en la siguiente figura:



Configuración de la red LAN.

Las interfases del switch deberán ser conectadas apropiadamente para que se establezca la adecuada comunicación entre todos los host.
Como se ha venido haciendo en prácticas anteriores, se debe establecer las direcciones IP en la interfase del ruteador y en cada uno de los host, para lograr una apropiada conectividad en la red LAN.

Anotar el plan de numeración IP en la tabla 1:

Tabla 1

Dispositivo	Interfase	Dirección IP	Clase
Ruteador			
Switch			
Pc 1			
Pc 2			
Pc 3			

Comprobar que se está recibiendo la señal en cada una de las Pc's, emitiendo señales de eco a cada dirección IP que conforma la red y verificar la configuración de cada una de las interfases que se están configurando por medio de comando correspondiente.

Para configurar la interfase Fast Ethernet del ruteador se tiene que ingresar a la interfase la cual esta conectada al switch y asignarle una dirección IP y su máscara, no olvidar dar de alta el enlace entre estos dos dispositivos.

Verificar que la correcta configuración del puerto Ethernet en el ruteador se ha completado satisfactoriamente, en este punto tendrá que observarse en la pantalla del ruteador que el protocolo se encuentra levantado, así como la interfase.

Mandar señales de eco a todas las direcciones IP desde el ruteador y de cada uno de los host de la red LAN para verificar su conectividad y ver la tabla de direcciones MAC en el switch.

Anotar los comandos que se requieren en la implementación y verificación de la red LAN en la tabla 2

Tabla 2

Comando	Descripción

Cuestionario:

1. Elabore un esquema detallado de la topología de la red LAN, señalando las interfases que se usaron y las direcciones IP.

2. ¿Cual es el comando que se usa para ver la correcta configuración de la interfase Ethernet? Muestre como aparece la información en pantalla.

3. ¿Cual es el comando usado para ver la configuración IP en el switch?

4. ¿Se podrían unir dos redes LAN como la anterior sin el uso del ruteador y en su lugar otro switch? Explique como y que precauciones se deben tomar.

5. Suponiendo que el ruteador tuviera conexión hacia una red externa, ¿La numeración IP empleada para esta red LAN sería la apropiada, que problemas se presentarían y como podrían solucionarse.

Cuestionario preliminar de la práctica 3

¿Que son las señales de eco y como se usan en una red?

¿Cuál es la tarea de un concentrador (Hub) y que diferencias tiene con un switch y un puente?

¿Cómo funciona un LAN switch y que medios usa para lograr la comunicación en la red?

¿Cuáles son las topologías mas comúnmente usadas en las redes LAN

¿Cuáles son los principales estándares LAN?

¿Como funciona CSMA/CD?

Práctica 4 Subnetting y Ruteo

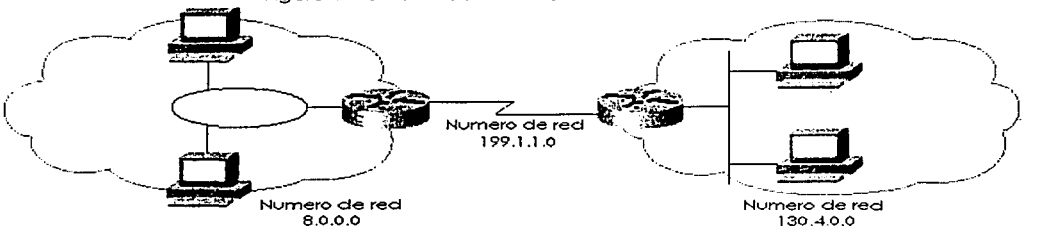
Introducción:

- Clases de Redes

Las clases de redes A, B, y C proporcionan tres tamaños de red. Por definición, todas las direcciones en la misma red, tienen el mismo valor numérico en la porción de red de las direcciones. El resto de la dirección se llama la porción del host de la dirección. Las direcciones individuales en la misma red, tienen todas un valor diferente en la parte del host de las direcciones, pero tienen valores idénticos en la parte de red.

Las redes clase A tienen una parte de red de 1 byte de longitud. Eso deja 24 bits para el resto de la dirección, o la parte del host. Eso significa que 2^{24} direcciones son numéricamente posibles en una red clase A. Semejantemente, las redes clase B tienen una parte de red de 2 bytes de longitud, dejando 16 bits para la porción del host de la dirección. Así que, existen 2^{16} posibles direcciones en una sola red clase B. Finalmente, las redes clase C tienen una parte de red de 3 bytes de longitud, dejando sólo 8 bits para la parte del host que implica sólo 2^{8} direcciones en una red clase C

Figura 1 Números de identificación de cada red



Los números de red se parecen a las direcciones (en el formato decimal punteado), pero no son asignables a cualquier interfase como una dirección de IP. Conceptualmente, los números de red representan el grupo de todas las direcciones IP en la red. Numéricamente, el número de red se construye con un valor diferente de cero en la parte de red, y con ceros en la parte del host del número de red, como se muestra en la figura 1.

Tabla 1

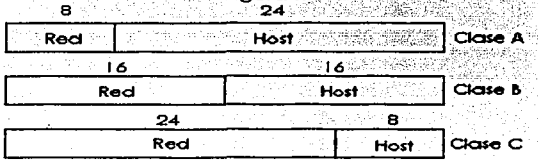
Clase	Rango del primer octeto	Números de red válidos	Numero total de esta clase de red	Número de host por red
A	1 a 126	1.0.0.0 a 126.0.0.0	2^{7} menos dos casos especiales	2^{24} menos dos casos especiales
B	128 a 191	128.1.0.0 a 191.254.0.0	2^{14} menos dos casos especiales	2^{16} menos dos casos especiales
C	192 a 223	192.0.1.0 a 223.255.254.0	2^{21} menos dos casos especiales	2^{8} menos dos casos especiales

La columna de números de red válida, muestra los números de red reales. Hay varios casos reservados. Por ejemplo, la red 0.0.0.0 (disponible para el uso como una dirección broadcast) y 127.0.0.0 (disponible para el uso como la dirección del bucle de regreso) están reservadas. Las redes 128.0.0.0, 191.255.0.0, 192.0.0.0, y 223.255.255.0 también son reservadas.

- Máscaras y Formatos de Dirección IP

La máscara de la subred se usa para varios propósitos. Un tema importante es definir el número de bits del host en una dirección. Esta máscara se usa por las computadoras al calcular la red o número de subred de la cual esa dirección es miembro.
Para apreciar totalmente para que se usa la mascara, se debe entender el formato de una dirección IP. La figura 2 muestra el formato de direcciones clase A, B, y C, cuando no se usa el subnetting.

Figura 2



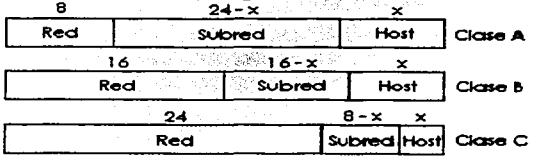
La máscara predefinida usada con cada clase de red, define el número de bits del host. La máscara tiene el número binario 0 para cada posición de bit correspondiente en la dirección que se considera que es parte de la porción del host de la dirección. La máscara implica el tamaño y posición de la parte de red de la dirección; sin embargo, la parte de red de hecho ya esta implicada por la clase de red. La tabla 2 resume las máscaras predefinidas y refleja los tamaños de las dos partes de una dirección IP.

Tabla 2

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

Cuando se usa el subnetting, aparece una tercera parte de una dirección IP, llamada la parte de subred de la dirección. Este campo se crea "robando" bits de la parte del host de la dirección. La figura muestra el formato de las direcciones cuando se usa el subnetting.
Ahora existen tres porciones de la dirección: la red, subred, y el host. El tamaño de la parte de red es determinado por la clase (A, B, o C). La parte del host es determinada por la mascara de la subred en uso, el número de bits de valor 0 en la mascara de la subred define el número de bits del host. Los bites restantes definen el tamaño de la parte de la subred de la dirección. Por ejemplo, una máscara de 255.255.255.240, usada con una red clase C, implica cuatro bits del host. Como se muestra en la figura 3, una red clase C tiene 24 bits de red. La mascara tiene cuatro 0s binarios al final, implicando 4 bits del host.

Figura 3



El número de host por red o subred se define por el número de bits del host; $2^{hostbits}$ menos dos casos especiales reservados, es el número de direcciones IP asignables en una red o subred. Semejantemente, el número de subredes de una red, asumiendo que la misma mascara se usa en todas las subredes, se define por el número de bits de la subred; 2 bits de la subred es el número de subredes IP utilizables de esa red. Dos casos especiales, la "subred cero" y la "subred broadcast" eran reservados en el pasado pero ahora son utilizables.

- Enrutamiento o Ruteo

La función primordial de una red de conmutación de paquetes es aceptar paquetes procedentes de una estación emisora y enviarlos hacia una estación de destino. Para ello se debe determinar una ruta o camino a través de la red, siendo posible generalmente la existencia de más de uno. Así pues, se debe realizar una función de enrutamiento.

- Estrategias de enrutamiento

Existen numerosas estrategias de enrutamiento para abordar las necesidades de ruteo en las redes de conmutación de paquetes. Muchas de ellas son aplicables también al enrutamiento en la interconexión de redes.

- Ruteo estático

En el enrutamiento estático se configura una ruta única y permanente para cada par de nodos origen-destino en la red. Pudiéndose utilizar para ello cualquiera de los algoritmos de enrutamiento. Las rutas son fijas, o al menos mientras lo sea la topología de la red. Así los costes de enlace usados para el diseño de las rutas no pueden estar basados en variables dinámicas tales como el tráfico, aunque si podrían estarlo en tráfico esperado o en capacidad.

- Ruteo dinámico

Prácticamente en todas las redes de conmutación de paquetes se utiliza también un tipo de técnica de enrutamiento adaptable; es decir, las decisiones de enrutamiento cambian en medida que lo hacen las condiciones de la red.

- Protocolos de ruteo

En un conjunto de redes, los dispositivos de enrutamiento son responsables de recibir y reenviar los paquetes a través del conjunto de redes interconectadas. Cada dispositivo de enrutamiento realiza la decisión de enrutamiento basándose en el conocimiento que se tiene sobre la topología y las condiciones del conjunto de redes. En un conjunto de redes sencillo, es posible utilizar un esquema de enrutamiento fijo, en conjuntos de redes más complejos, se necesita un grado de cooperación dinámica entre los dispositivos de enrutamiento. En particular, se deben evitar aquellas porciones de red que han sufrido un fallo y se deberían evitar aquellas porciones de red que sufren congestión. Para poder tomar estas decisiones de enrutamiento dinámicas, los dispositivos de enrutamiento deben intercambiar información de enrutamiento usando un protocolo de enrutamiento especial para ese propósito. La información que se necesita sobre el estado del conjunto de redes tiene que venir expresada en términos de qué redes son accesibles a través de que dispositivos de enrutamiento y en términos de las características en retardo de varias rutas

- Comparando los Protocolos de Ruteo

Existen varios protocolos de ruteo para TCP/IP. La larga historia de IP y su continua popularidad han requerido la especificación y creación de varias opciones. Así que, es útil clasificar los protocolos de ruteo IP basándose en sus diferencias.

Una mayor clasificación de los protocolos de ruteo IP, es si ellos están optimizados para crear las rutas dentro de una organización o rutas entre dos o más organizaciones interconectadas. Los protocolos de ruteo exteriores están optimizados para usarse entre ruteadores de diferentes organizaciones. El Protocolo de Entrada de la frontera (Border Gateway Protocol - BGP) y el Protocolo de la Entrada Exterior (Exterior Gateway Protocol - EGP) son las dos opciones para los protocolos de ruteo exteriores; BGP es el más popular y el más recientemente desarrollado de los dos. (EGP no es técnicamente un protocolo de ruteo; está obsoleto.)

El termino protocolo de ruteo es el término usado para describir los programas y procesos usados para intercambiar y aprender información de ruteo. Otros documentos llaman a estos mismos programas y procesos "algoritmos de ruteo".

- Ruteo de vector de distancia

Los especialistas en redes trabajan a diario con problemas de ruteo; algunos de estos problemas son resultado de la lógica detrás del vector de distancia que los protocolos de ruteo. Para entender que significa el vector de distancia se necesita entender como un protocolo de ruteo logra sus siguientes metas:

- Aprender información de ruteo
- Notificar rutas fallidas
- Agregar las mejores rutas actuales después de que una ha fallado
- Prevenir las vueltas

Los protocolos de ruteo de vector de distancia aprenden y anuncian rutas. Las rutas puestas en la tabla de ruteo deben ser libres de vueltas y deben ser las rutas conocidas que funcionen mejor. La métrica se usa para escoger la mejor ruta. Mecanismos tales como el horizonte partido y tiempos de espera se usan para prevenir las vueltas de ruteo.

Tabla 6-13 IP RIP e IGRP EXEC

Comando	Función
show ip route [*subred*]	Muestra toda la tabla de ruteo, o una entrada si se introduce la subred
show ip protocol	Muestras los parámetros del protocolo de ruteo y los valores actuales del cronometro
debug ip rip	Emite mensajes log para cada actualización RIP
debug ip igrp transactions	Emite mensajes log con detalles de las actualizaciones IGRP
debug ip igrp events	Emite mensajes log para cada paquete IGRP
Ping	Envía y recibe mensajes de eco ICMP para verificar la conectividad
trace	Envía una serie de ecos ICMP con valores TTL crecientes para verificar la ruta actual a un host

- El comando network

Cada comando **network** habilita RIP o IGRP en un conjunto de interfases. El comando **network** causa la implementación de las siguientes tres funciones:

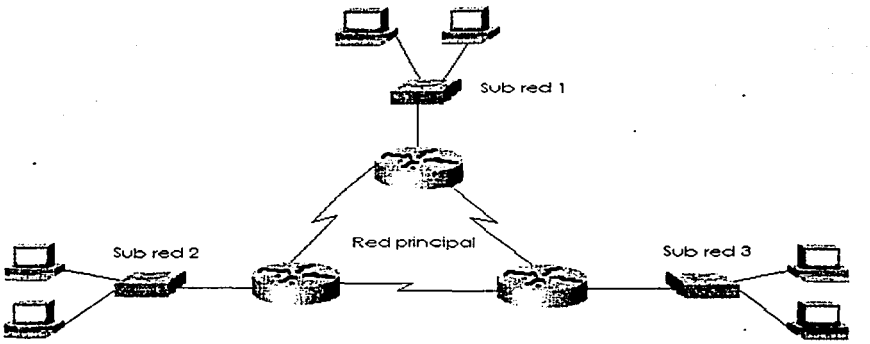
- Las actualizaciones de ruteo son transmisiones o multitransmisiones fuera de una interfase.
- Las actualizaciones de ruteo son procesadas si ellas entran en esa misma interfase.
- La subred directamente conectada a esa interfase es anunciada.

El comando **network** coincide con algunas de las interfases configuradas en un ruteador. Las interfases que se configuran con el comando **network** y que forman parte de una misma red, tienen las tres funciones previamente mencionadas las cuales se realizan en ellas.

El comando **show ip route** tiene varias opciones que serán útiles al arreglar una red grande. El comando **Ip show protocol** también puede proporcionar alguna información muy útil al arreglar un problema de ruteo. Con una red pequeña, la mayoría de las opciones en el comando **show ip route** son innecesarias. Sin embargo, sabiendo las opciones y lo que cada uno puede hacer será muy útil para su trabajo con redes más grandes.

- Desarrollo de la práctica

En esta práctica se implementara el plan de numeración IP de la red que se muestra a continuación, tomando en cuenta que se debe hacer el subnetting para que la red tenga un funcionamiento apropiado.
Para esta práctica se debe abrir el simulador, y en la pantalla inicial, se debe escoger la opción de "cargar la utilidad de diseño de red" para establecer la red que se muestra en la figura; seleccionando ruteadores del modelo 2500 y switches de la serie 1900, teniendo cuidado en la forma en la cual se van a configurar las interfases.



Para una mejor planeación, guiándose con la figura anterior, establecer las direcciones IP en la siguiente tabla:

Dispositivo	Interfase	Dirección	Máscara	No. de red
Ruteador 1	Ethernet 0			
	Serial 0			
	Serial 1			
Ruteador 2	Ethernet 0			
	Serial 0			
	Serial 1			
Ruteador 3	Ethernet 0			
	Serial 0			
	Serial 1			
Switch 1	PC 1			
	PC 2			
Switch 2	PC 1			
	PC 2			
Switch 3	PC 1			
	PC 2			

En cada una de las tres redes formadas por el ruteador, el switch y las dos PC's, se debe comprobar que existe la comunicación entre cada uno de los dispositivos enviando mensajes de eco ICMP por medio del comando **ping**.

Comprobando que en cada una de las tres redes la conectividad esta establecida, se procederá ahora a unirlas para formar una red con tres subredes, por medio del comando **route**, el cual activará el ruteo, establecerá las tablas de ruteo y se transmitirán entre los tres ruteadores para permitir la comunicación entre las PC's.

Configurando entre las interfases seriales de los ruteadores un enlace con encapsulamiento, HDLC (El cual es el predeterminado en los ruteadores de Cisco), lo siguiente es establecer la numeración IP de la red principal en las interfases y verificar la comunicación entre ellos. Llevando a cabo lo anterior y verificando la comunicación, lo que resta ahora es habilitar el ruteo.

Para establecer el ruteo, se ingresa al modo de configuración global y al emitir el comando **"?"** de ayuda, se despliegan los comandos disponibles en ese modo, de entre los cuales se puede apreciar el comando **router**. Las opciones que se tienen para los protocolos de ruteo son las siguientes:

```
Router(config)#router ?

eigrp           Enhanced Interior Gateway Routing Protocol (EIGRP)
igrp            Interior Gateway Routing Protocol (IGRP)
ospf            Open Shortest Path First (OSPF)
rip             Routing Information Protocol (RIP)
```

Seleccionando el ruteo **igrp** se tiene que dar un número de identificación de red, el cual se llama sistema autónomo, y sirve para que las tabas de ruteo solo se compartan con los ruteadores que sean de ese mismo sistema autónomo. Estando en el modo de ruteo, se emite el comando **network** para anunciar las redes clase B en ese ruteador:

```
Router(config)#route igrp 100
Router(config-router)#
Router(config-router)#network 172.16.0.0
Router(config-router)#network 172.16.0.0
Router(config-router)#
```

Al verificar la configuración del proceso de ruteo se tiene que emitir el comando **show ip route** para que el sistema operativo muestre la información acerca de las tabas de ruteo en cada ruteador, mostrando de que direcciones están siendo anunciadas a los otros ruteadores, aquí un ejemplo de una tabla de ruteo:

```
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,
       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

Gateway of last resort is not set
C 172.16.0.0/16 is directly connected, 172.16.1.2
```

Por último comprobar que se esta llevando a cabo el ruteo enviando mensajes de eco desde cada uno de las PC´s entre cada una de ellas. Con esto se comprobará que la numeración IP se estableció correctamente en las subredes y que el ruteo se esta completando correctamente.

- Cuestionario:

1. ¿Como se llevo a cabo el ruteo en esta práctica y que tipo de ruteo es?
2. ¿De la numeración IP que se escogió, cuantas subredes y cuantos host son posibles?. Escriba el procedimiento.
3. ¿Cuál es el propósito del número de identificación de red cuando se habilita eigrp?
4. ¿Cuál es el proceso a seguir para establecer una red alterna entre el ruteador 1 y el ruteador 3?
5. ¿Se podría asignar una numeración IP diferente a cada subred?

Cuestionario preliminar de la práctica 4

Para el desarrollo de la práctica 4, se requiere que el alumno resuelva el siguiente cuestionario:

¿Qué son las direcciones IP?

¿Cuál es el problema de disponibilidad de direcciones IP con la numeración IPv4?

¿Qué es el subnetting y como se emplea?

De un ejemplo de subnetting

¿Cuál es el motivo de que haya direcciones no válidas?

¿De cuántas partes se divide una dirección "subneteada"?

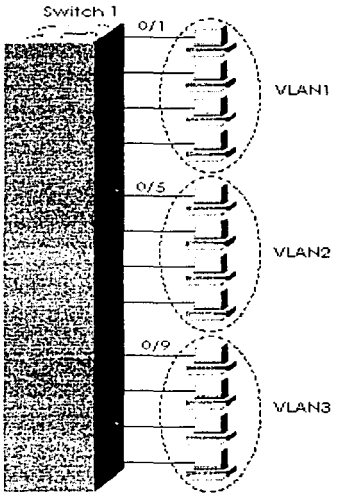
¿Cómo se puede implementar la numeración IP

Práctica 5 Redes Lan Virtuales

Introducción

- LANs virtuales

Una LAN virtual (VLAN) es un dominio de transmisión creado por uno o más switches. La VLAN se crea por medio de la configuración en el switch. Si un diseño de red requiere de tres dominios de transmisión separados, podrían usarse tres switches para cada dominio de transmisión. Cada switch también se conectaría a un ruteador para que los paquetes puedan rutearse entre los dominios de transmisión. En cambio, usando VLANs, podría usarse un switch el cual manejaría tres juegos diferentes de puertos así como también tres dominios diferentes de transmisión.



Puede haber varias VLANs definidas en un solo switch. Una VLAN también puede constar de múltiples switches. Usando protocolos de capa 2 como el IEEE 802.1q e ISL (Enlace de switch interno) le permite a una VLAN extenderse a través de múltiples switches. Las VLAN se forman para agrupar a los usuarios relacionados sin tener en cuenta las conexiones físicas de sus host hacia la red. Los usuarios pueden extenderse por una red de campus o incluso por locaciones geográficamente aisladas. Pueden organizarse los usuarios en VLANs separadas según su sección, departamento, locación, función, aplicación, dirección (lógica o física), o el protocolo usado.
La meta con las VLANs, es agrupar a los usuarios en VLANs separadas para que su tráfico se quede dentro de la VLAN. Cuando se configuran VLANs, la red puede aprovecharse de los siguientes beneficios:

- Con las VLANs, movimientos, sumas, y cambios en las conexiones de los dispositivos son más fáciles.
- Obligando al dispositivo de ruteo de capa 3 a involucrarse entre VLANs, puede usarse un mayor control administrativo (mejor conteo, listas de acceso, y así sucesivamente).
- El consumo innecesario del ancho de banda LAN es reducido comparado con un solo dominio de transmisión.
- El uso innecesario del CPU es reducido por el resultado de la reducción de la transmisión remitida.

- Configuración básica de VLAN

En esta sección se discuten las pautas para configurar VLANs en el switch Cisco 1900. Se deben recordar varias cosas antes de empezar con la configuración VLAN:

- El número máximo de VLANs depende del switch. El Catalyst 1900 soporta 64 VLANs con un árbol de expansión separado por VLAN.
- VLAN1 es un valor predeterminado de fábrica VLANs.
- Se envían anuncios CDP y VTP en la VLAN1.
- La dirección IP del Catalyst 1900 está en el dominio de transmisión de la VLAN1.
- El switch debe estar en el modo de servidor VTP para crear, agregar, o borrar VLANs.

- El Protocolo Troncal VLAN (VTP)

VTP es un protocolo usado entre los switches para simplificar el manejo de las VLANs. Con el VTP, se puede hacer cambios de configuración centralmente, en un solo switch de la serie Catalyst y tales cambios se hacen automáticamente, comunicándose a todos los otros switch en la red. VTP es un protocolo de mensajería de capa 2 que mantiene la consistencia de la configuración de la VLAN manejando la incorporación, el borrado, y el cambio de nombre de las VLANs. VTP minimiza las inconsistencias de configuración que pueden producir varios problemas, como nombres de VLAN dobles, especificaciones de tipo de VLAN incorrectas, y violaciones de seguridad.

Desarrollado por Cisco, es la primera implementación de protocolo de la industria específicamente diseñada para despliegues de VLAN grandes. VTP refuerza el despliegue de VLAN proporcionando lo siguiente:

- La integración de ISL, 802.10, y ATM base LAN VLANs.
- Auto-inteligencia dentro de los switches para configurar VLANs.
- Consistencia de configuración a través de la red.
- Un esquema de auto-mapeo para ir a través de troncales mixtas.
- Rastreo exacto y monitoreo de VLANs.
- Reporte dinámico de VLANs agregadas a través de la red.
- Set up Plug and Play y configuración cuando se agregan nuevas VLANs

Existen tres modos de operación del VTP

Servidor — Es el modo Predefinido para todos los switches Catalyst. Se necesita por lo menos uno para propagar los datos VLAN a lo largo del dominio.

Cliente — Recibe la información de los servidores VTP y envía y recibe las actualizaciones, pero no puede hacer ningún cambio.

Transparente No participa en el dominio VTP, pero continuara remitiendo los anuncios VTP a través de los enlaces troncales configurados.

Lista de comandos VLAN

Comando	**Descripción**
delete vtp	Restablece todos los parámetros VTP a los valores predefinidos y restablece el número de revisión de configuración a 1
vtp [server | transparent | client] [domain *dominio-nombre*] **[trap {enable | disable}] [password** *contraseña*] **[pruning {enable | disable}]**	Define los parámetros VTP
vtp trunk pruning-disable *vlan-lista*	Desactiva el recorte para específicas VLANs en una interfase troncal en particular (subcomando de la interfase)
show vtp	Despliega el estado del VTP
trunk [on | off | desirable | auto | nonegotiate]	Configura una interfase de la troncal
show trunk	Despliega el estado de la troncal
vlan #*vlan* **name** *nombre vlan*	Define una VLAN y su nombre
show vlan	Despliega la información de la VLAN
vlan-membership static *vlan#*	Asigna un puerto a una VLAN
show vlan-membership	Despliega el número de miembros de la VLAN
show spantree *vlan#*	Despliega la información del árbol de expansión para una VLAN

Beneficios del uso de VLANs

- Control de transmisión(Broadcast)

Así como los switches aíslan físicamente los dominios de colisión para los host conectados y sólo envían el tráfico fuera de un puerto en particular, las VLANs refinan este concepto más allá y proporcionan el aislamiento completo entre VLANs. Una VLAN es un dominio puenteado, y todo el tráfico broadcast y multicast esta contenido dentro de él.

- Seguridad

Las VLANs proporcionan seguridad de dos maneras:

Pueden agruparse los usuarios de alta seguridad en una VLAN, posiblemente en el mismo segmento físico, y ningún usuario fuera de esa VLAN puede comunicarse con ellos.

Debido a que las VLANs son grupos lógicos que se comportan como entidades físicamente separadas, la comunicación VLAN interna, sólo puede lograrse a través de un ruteador. Cuando la comunicación VLAN interna ocurre a través de un ruteador, puede usarse toda la seguridad y la funcionalidad de filtrado que los ruteadores proporcionan tradicionalmente. En el caso de protocolos no ruteables, puede no haber ninguna comunicación VLAN interna. Toda la comunicación debe ocurrir dentro de la misma VLAN.

- Rendimiento

  Se puede aislar usuarios que requieran de redes de alto rendimiento para proyectos de ancho de banda intensivo, las VLANs pueden aislarlos del resto de la red.

- Manejo de la red

  El Software en el switch le permite asignar usuarios a las VLANs y, después, reasignarlos a otra VLAN. El recableado para cambiar la conectividad ya no es necesario en el ambiente de switcheo LAN, porque las herramientas de dirección de red lo permiten lógicamente al reconfigurar la LAN en segundos.

Predefinidamente los ruteadores sólo envían las transmisiones dentro de la red original, pero los switch las remiten a todos los segmentos. Esto se conoce como una red plana porque es un dominio de transmisión grande. Los switches y las VLAN son usadas para reemplazar la red plana. Todos los miembros de una VLAN están en el mismo dominio de transmisión y reciben todas las transmisiones. Predefinidamente las transmisiones se filtran de todos los puertos en un switch que no está en la misma VLAN. Los ruteadores, switches de capa 3, o Módulos de Switch de Ruta (RSM) debe usarse junto con los switch para proporcionar las conexiones entre las redes (VLANs), las cuales pueden detener las transmisiones de la propagación a lo largo de toda la red interna.

- Comunicación entre VLANs

Para comunicarse entre VLANs se necesita tener un ruteador con una interfase para cada VLAN o un ruteador que soporte el ruteo ISL. El ruteador de Cisco más bajo que soporta el ruteo ISL es la serie 2600. Si se está usando un ruteador con una interfase e ISL, la interfase debe ser por lo menos 100Mbps (Fast Ethernet).

- Organizaciones de VLAN

Cada nodo conectado a la red física necesita tener el mismo número de red para comunicarse en la red interna. En los switches es posible puede agrupar a los usuarios en las comunidades de interés, llamadas Organizaciones VLAN. En una VLAN, los nodos de la red de cada VLAN pueden comunicarse con otros nodos en la misma VLAN, los nodos en una VLAN necesitan pasar por un ruteador u otro dispositivo de capa 3 para comunicarse con otras VLAN.
Las VLANs normalmente son creadas por administradores que asignan los puertos del switch a las VLANs. Estas se llaman VLANs estáticas. Las VLANs dinámicas son configuradas asignando todas las direcciones de hardware de los dispositivos del host en una base de datos.

VLAN Estática - Las VLANs estáticas son el método típico de creación de las VLANs y son las más seguras. El puerto del switch el cual fue asignado una asociación VLAN, mantiene siempre esa asociación hasta que el administrador de la red cambia la asignación del puerto.

VLAN Dinámica - Las VLANs dinámicas determinan la asignación VLAN de un nodo automáticamente. Usando software de manejo inteligente, se puede habilitar direcciones MAC, protocolos, o incluso aplicaciones para crear VLANs dinámicas. Por ejemplo, si la dirección MAC está en una base de datos centralizada, y si se conecta hacia un puerto del switch, la base de datos de manejo de VLAN puede mirar la dirección y configurar el puerto para la VLAN correcta. Si el usuario se mueve, el switch asignará el puerto automáticamente a su VLAN correcta.

- Enlaces en un Ambiente Switcheado

Las VLANs pueden abarcar múltiples switches conectados usando el etiquetaje de trama y conexiones troncales. Los switch deben mantener un rastreo de las tramas y a que VLAN pertenece

la trama. El etiquetaje de trama realiza esta función. Los switches pueden entonces dirigir las tramas hacia el puerto apropiado.

- Enlaces de acceso

A los enlaces que son sólo parte de una VLAN se les hace referencia como la VLAN nativa del puerto. Cualquier dispositivo vinculado a un enlace de acceso es desprevenido de una membresía VLAN. Este dispositivo solo asume que es parte de un dominio de transmisión, sin ninguna comprensión de la red física. Los switches quitan cualquier información VLAN antes de que se envíe a un dispositivo de enlace de acceso. Los dispositivos de enlace de acceso no pueden comunicarse con cualquier dispositivo fuera de su VLAN sin un ruteador o dispositivo de capa 3

- Enlaces troncales

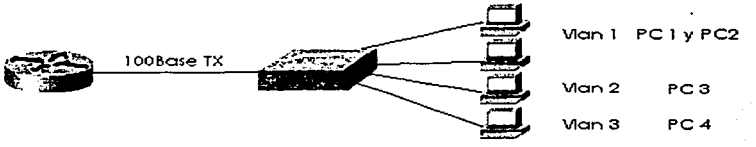
Las troncales pueden llevar múltiples VLANs y son usadas para conectar los switches a otros switch, ruteadores, o servidores. Los enlaces troncales sólo son soportados en enlaces Fast o Gigabit Ethernet (100 o 1000 Mbps). Los switches Cisco soportan dos formas de identificar a qué VLAN pertenece una trama: ISL y 802.1q. Si no se especifica ningún tipo de encapsulamiento troncal al configurar una troncal Ethernet, ISL se usa como valor predefinido. Los enlaces troncales tienen una VLAN nativa o predefinidos que se usa si falla el enlace troncal. Los enlaces troncales llevan el tráfico de múltiples VLANs de 1 a 1005 al mismo tiempo. Las troncales le permiten hacer de un solo puerto, una parte de múltiples VLANs, por lo que se puede estar en más de un dominio de transmisión a la vez. Cuando se conectan switches juntos, los enlaces troncales pueden llevar alguna o toda la información a través del enlace de VLAN. Si no hiciera troncal el enlace, entonces el switch llevará sólo la información de la VLAN 1 a través del enlace. Los switches de Cisco usan el Protocolo de Troncales Dinámico (DTP - Dynamic Trunking Protocol). DTP es un PPP que fue creado para enviar la información de la troncal a través de troncales 802.1q

Tronqueo

Enlace de switch interno (ISL - Inter Switch Link) es un protocolo propiedad de Cisco para interconectar múltiples switches y manteniendo la información VLAN como tráfico circulante entre los switches. ISL es similar a 802.10 cuando ambos grupos de puentes multiplexados sobre una troncal de alta velocidad (ISL sólo corre en Fast Ethernet). Con ISL, una trama Ethernet se encapsula con una cabecera que mantiene las VLAN ID entre los switches. Una cabecera de 26 bytes que contiene una VLAN ID de 10 bits esta predestinado a la trama Ethernet. Un VLAN ID sólo se agrega a la trama cuando la trama se destina para una red no local. Desde que la trama se encapsula, sólo dispositivos que corran ISL pueden leerla. Si se necesita un protocolo para Switch que no sean Cisco, use el 802.1q. Las tramas ISL pueden ser hasta 1522 bytes largo. En puertos multi VLAN, cada trama se etiqueta como entran en el switch. Los ISL NICs permiten a los servidores enviar y recibir tramas etiquetadas con VLANs múltiples para que las tramas puedan cruzar las VLANs múltiples sin pasar por un ruteador. El protocolo ISL puede permitirle a un servidor de archivos existir en VLANs múltiples al mismo tiempo. Note que el encapsulamiento ISL sólo se agrega a tramas que se remiten en un enlace troncal, y cuando ellas llegan al enlace de acceso, el encapsulamiento se quita y la trama se entrega.

Desarrollo de la práctica:

Para el desarrollo de esta práctica, se requiere que se diseñe una red como la que se muestra en la figura. En esta red la cual cuenta con cuatro host, se establecerán tres Vlans, dos PC´s en una Vlan y cada una de las dos PC´s en una Vlan por separado para obtener tres redes LAN virtuales.



Abriendo el simulador en la opción de diseño de red, se debe seleccionar un ruteador y un switch con capacidad para configurar Vlans, para configurar la red de la figura anterior, estableciendo sus interfases apropiadamente

Habilitar la red como se ha implementado en prácticas anteriores y comprobar la comunicación entre todas las PC´s entre si, con el switch y el ruteador.

Para el enlace troncal entre el ruteador y el switch, es necesario habilitar el enlace como full duplex y con encapsulamiento ISL.

Dispositivo	Dirección IP	Comunicación con todos los dispositivos?	No hay comunicación con:
PC 1			
PC 2			
PC 3			
PC 4			
Switch			
Ruteador			

Comprobando lo anterior, se dispondrá a habilitar una red virtual de la siguiente manera:

Dar de alta el protocolo troncal VLAN (VTP) en el modo de servidor, por medio del comando de configuración **vtp**. Emitir el comando de ayuda para desplegar en la pantalla las opciones que se tienen con el protocolo troncal VLAN, y elegir la opción server.

A continuación, se deberán crear las redes virtuales, a las cuales se debe especificar un número y un nombre para un mejor control.

```
Switch#configure terminal
Switch(config)#vtp server
Switch(config)#

Switch(config)#vlan 2 name nombre de la Vlan
Switch(config)#vlan 3 name nombre de la Vlan
Switch(config)#
```

Por último, se designa el puerto para cada red virtual y se le asigna un número de identificación de Vlan, con el propósito de establecer tres redes virtuales, las cuales costaran de 2 PC's en la red 1, una PC en la red 2 y otra en la red 3
Esto se logrará hacer por medio del comando **vlan-membership**, el cual asigna un número de red a un puerto en el switch:

```
Switch(config)#interface Ethernet 0/3
Switch(config)#vlan-membership static 2
```

Para verificar que se llevo a cabo la configuración correctamente, se emplea el comando **sh vlan-membership**, el cual nos muestra la información relacionada con los puertos y a que red pertenecen. Para la configuración de la troncal en el ruteador, se tiene que habilitar tres subinterfases en la interfase Fast Ethernet, con esto se logrará la comunicación entre las tres redes y el ruteador.

```
Router#configure terminal
Router(config)#interface FastEthernet 0/0.1
Router(config-subif)#encapsulation isl 1
Router(config-subif)#
```

Este proceso se tiene que llevar a cabo en las tres sub interfases Fast Ethernet. A continuación se verificará la comunicación entre todos los dispositivos y se anotará en la tabla siguiente:

Dispositivo	Dirección IP	Num. De red virtual	Com. con todos los dispositivos?	No hay señal de retorno con:
PC 1				
PC 2				
PC 3				
PC 4				
Switch				
Ruteador				

Cuestionario:

¿Cuál es la diferencia de usar VLANs y usar la red switcheada convencional?

¿Que beneficios se obtienen al configurar redes LAN virtuales?

Mencione un ejemplo de aplicación de una red VLAN en base a su funcionalidad

¿Cómo se lleva a cabo el ruteo entre las redes VLAN?

¿Cómo es la implementación de la numeración IP entre las redes VLAN?

¿Qué hubiera pasado si no se habilita en el ruteador la troncal con el switch?

¿Por qué se tuvieron que habilitar tres subinterfases en el ruteador?

Cuestionario preliminar de la práctica 5

Para desarrollar la práctica 5 se requiere resolver el siguiente cuestionario:

¿Qué es una red LAN virtual?

¿Que beneficios se obtienen al implementar una red VLAN?

¿Qué protocolo se usa entre las redes VLAN?

¿Cómo es la seguridad entre estas redes?

¿Qué interfase se usa del switch hacia el ruteador cuando se usan redes LAN?

¿A que se refiere la norma IEEE 802.1q?

Práctica 6 Protocolo punto a punto

Líneas Arrendadas punto a punto

Un enlace punto a punto proporciona una sola forma de ruta de comunicaciones WAN preestablecida a través de una red troncal, como una compañía telefónica, hacia una red remota. Un enlace punto a punto también se conoce como una línea arrendada, porque su camino establecido es permanente y fijo para cada red remota alcanzada a través de las instalaciones del portador.

Los protocolos WAN usados en los enlaces seriales punto a punto proporcionan la función básica de la entrega de datos a través de ese enlace. Los protocolos WAN tienen las siguientes funciones en común:

- LAPB, HDLC, y PPP proveen la entrega de datos a través de un solo enlace serial punto a punto.
- LAPB, HDLC, y PPP entregan los datos en los enlaces seriales síncronos. (PPP soporta las funciones asíncronas también.)

Los enlaces síncronos, se usan típicamente entre los ruteadores en lugar de los enlaces asíncronos.

Protocolo Punto a Punto PPP

El protocolo Punto a Punto es un protocolo estandarizado de la industria el cual puede ser usado para crear los enlaces punto a punto entre los diferentes equipos del usuario.

Atributos del protocolo de enlace de datos punto a punto

Protocolo	¿Corrección de error?	¿Campo de tipo de arquitectura?	Otros atributos
Synchronous Data Link Control (SDLC)	Si	Nulo	SDLC soporta enlaces multipunto: asume que la cabecera SNA ocurre después de la cabecera SDLC.
Link Access Procedure Balanced (LAPB)	Si	Nulo	La especificación asume un solo protocolo configurable después de LAPB. LAPB se usa principalmente con X.25. Cisco usa un campo de tipo de propietario para soportar el tráfico del multiprotocolo.
Link Access Procedure on the D channel (LAPD)	No	No	LAPD no se usa entre los ruteadores, pero es usado en el canal D desde el ruteador hacia el switch ISDN para la señalización
High-Level Data Link Control (HDLC)	No	No	HDLC sirve como el valor predefinido de Cisco en los enlaces seriales. Cisco usa un campo de tipo de propietario para soportar el tráfico del multiprotocolo.
Protocolo punto a punto (PPP)	Le permite al usuario que escoja si la corrección de error se ha realizado. La corrección usa LAPB	Si	PPP se hizo para la interoperabilidad del multiprotocolo de su principio, al contrario de todos los otros. PPP también soporta la comunicación asíncrona.

El protocolo punto a punto, usa un campo de Protocolo de Control de Red en la cabecera de Enlace de Datos para identificar el protocolo de la capa de Red. Permite autenticación y conexiones multienlace y puede correr sobre enlaces asíncronos y síncronos.

El protocolo punto a punto es un protocolo de la capa de enlace de datos que puede usarse sobre enlaces asíncronos (dial-up) y seriales síncronos (ISDN) y usa el LCP (Protocolo de Control de Enlace) para construir y mantener las conexiones de enlace de datos. El propósito básico de PPP es transportar paquetes de capa 3 sobre un enlace punto a punto de capa de enlace de datos. PPP consiste en dos componentes principales, LCP (Protocolo de Control de Red) para establecer y configurar diferentes protocolos de capa de red. PPP está diseñado para permitir el uso simultáneo de múltiples protocolos de la capa de red.

- Configuración HDLC y PPP

Una tarea común para los expertos en redes, es habilitar un protocolo de enlace de datos de punto a punto apropiado. Con LAPB siendo la excepción. (Se debe estar seguro de configurar el mismo protocolo de enlace de datos WAN en cada extremo del enlace serie. De lo contrario, los ruteadores interpretarán mal las tramas entrantes, y el enlace no funcionara.). Las tablas 8-4 y 8-5 resumen los comandos de configuración y los comandos **show** y **debug** usados para la configuración HDLC y PPP.

Comandos show y de configuración PPP y HDLC

Comando	**Modo de configuración**
encapsulation {hdlc ppp lapb}	Subcomando de la interfase
compress Predictor | stac | mppc[ignore-pfc]]	Subcomando de la interfase
show interface	Lista las estadísticas y detalles de la configuración de la interfase, incluyendo el tipo de encapsulamiento.
show compress	Lista las proporciones de compresión.
show process	Lista el proceso y la utilización de tarea. Es útil cuando se mira el incremento de la utilización debido a la compresión.

El Protocolo de Control de Enlace

El Protocolo de Control de Enlace (LCP - Link Control Protocol) PPP proporciona las características básicas sin la necesidad de tener en cuenta el protocolo de capa 3 enviado a través del enlace. Una serie de protocolos de control PPP, como el Protocolo de Control IP (IP Control Protocol - IPCP), proporciona las características para un protocolo de capa en particular para funcionar bien a través del enlace.

Solo un LCP se necesita por enlace, pero se necesitan múltiples protocolos de control. Si un ruteador se configura para IPX, AppleTalk, e IP en un enlace serial PPP, el ruteador configurado para encapsulamiento PPP, automáticamente intenta plantear los protocolos de control apropiados para cada protocolo de capa 3. La tabla 8-6 resume las características de LCP las cuales realizan las funciones no específicas a una capa 3 en particular.

El LCP PPP proporciona un método de establecimiento, configuración, mantenimiento, y terminación de la conexión punto a punto. El LCP pasa por cuatro fases distintas.

1. Primero, ocurre el establecimiento del enlace y la negociación de la configuración. Antes de que cualquier datagrama de la capa de Red pueda intercambiarse (por ejemplo IP), primero, el LCP debe abrir la conexión y debe negociar los parámetros de la configuración. Esta fase está completa cuando una trama de reconocimiento de configuración ha sido enviadas y recibida.

2. Esto es seguido por la determinación de la calidad del enlace. LCP permite una fase de determinación de calidad del enlace opcional seguida por la fase de establecimiento del enlace y la negociación de la configuración. En esta fase el enlace se prueba para determinar si la calidad del enlace es suficiente para levantar los protocolos de la capa de red. Esta fase es optativa. LCP puede retrasar la información del protocolo de la capa de Red hasta que esta fase este completa.

3. Hasta este punto, ocurre la negociación de la configuración del protocolo de la capa de Red. Después de que LCP ha terminado la fase de determinación de la calidad del enlace, los protocolos de la capa de Red pueden ser configurados separadamente por el Protocolo de Control de Red apropiado y pueden levantarse y tirarse cuando se desee. Si el LCP cierra el enlace, informa a los protocolos de la capa de Red para que ellos pueden tomar la acción apropiada.

4. Finalmente, ocurre la terminación del enlace. EL LCP puede terminar el enlace en cualquier momento. Esto normalmente se hará a demanda del usuario, pero puede pasar debido a un evento físico, como la pérdida de la troncal o la expiración de un periodo ocioso del cronómetro.

El Protocolo de Control de Enlace ofrece diferentes opciones de encapsulamiento PPP, incluyendo las siguientes:

Autenticación - las opciones de la autenticación incluyen PAP y CHAP.
Compresión - la compresión de los datos aumenta la transferencia de datos en un enlace de red, reduciendo la cantidad de datos que deben transmitirse.
Detección de error - La calidad y los números Mágicos son usados por PPP para asegurar un enlace de datos fiable, libre de vueltas.
Multienlace - Soportado en el IOS 11.1 y posteriores, el multienlace es soportado en los enlaces PPP entre los ruteadores de Cisco. Esto divide la carga para PPP sobre dos o más circuitos paralelos y se llama bulto.

Características PPP LCP

Función	Numero de la característica LCP	Descripción
Detección de error	Monitoreo de la calidad del enlace (LQM)	PPP puede bajar un enlace basado en el porcentaje de errores en el enlace. LQM intercambia las estadísticas sobre los paquetes perdidos contra los paquetes enviados en cada dirección: cuando se comparan los paquetes y bytes enviados, esto rinde un porcentaje de tráfico erróneo. El porcentaje de pérdida que causa que un enlace sea bajado, es habilitado y definido por una colocación de la configuración.
Detección de enlace doblado	Número mágico	Usando un número mágico, los ruteadores envían mensajes entre si con un número mágico diferente. Si alguna vez recibe su propio número mágico, el enlace esta doblado. Un establecimiento de la configuración, determina si el enlace debe deshabilitarse cuando esta doblado.
Autenticación	PAP y CHAP	Mayormente usado en los enlaces de dial, PAP y CHAP pueden ser usados para autenticar el dispositivo en el otro extremo del enlace.
Compresión	STAC y predicción	Esta es compresión por software
Soporte multilink	Multilink PPP	Los fragmentos de paquetes son balanceados de carga a través de múltiples enlaces. Esta característica se usa más a menudo con dial. La sección "Multilink PPP" después en el capítulo, cubre este concepto en el detalle mayor.

Métodos de autenticación PPP

- Protocolo de Autenticación de contraseña (PAP - Password Authentication Protocol)

PAP Proporciona un método simple para un nodo remoto, para establecer su identidad usando un handshake bidireccional. Esto sólo se hace en el establecimiento de enlace de inicial. Después de que la fase de establecimiento del enlace PPP se completa, se envía un repetidamente un par de username/password por el nodo remoto hasta que la autenticación se reconozca, o la conexión se termina.

- Protocolo de saludo (handshake) y desafío (challenge) (CHAP)

CHAP es usado para verificar periódicamente la identidad del nodo remoto que usa un hanshake(saludo) de 3 vías. Esto se hace en el establecimiento del enlace inicial y puede repetirse en cualquier momento después de que el enlace se ha establecido. Después de que la fase de establecimiento del enlace PPP se completa, el host envía un mensaje de desafío al nodo remoto. El nodo remoto responde con un valor calculado usando una función hash de un sentido (típicamente MD5). El host verifica la contestación contra su propio cálculo del valor hash esperado. Si los valores coinciden, la autenticación se reconoce. De otra forma, la conexión se termina.

- Estableciendo la Autenticación PPP

Usar la autenticación con PPP es opcional, por consiguiente se debe configurar la autenticación PPP específicamente en cada host PPP para que el host utilice PPP.

CHAP y PAP se especifican en el RFC 1334. Estos protocolos son soportados en interfases serie síncronas y asíncronas. Al usar CHAP o autenticación PAP, cada ruteador se identifica por un nombre. Este proceso de identificación impide a un ruteador poner otra llamada hacia un ruteador al cual ya está conectado, y también previene el acceso desautorizado. El control de acceso usando CHAP o PAP está disponible en todas las interfases serie que usan el encapsulamiento PPP. La característica de autenticación reduce el riesgo de violaciones de seguridad en el ruteador. Se puede configurar CHAP o PAP para la interfase. Nótese que, para usar CHAP o PAP, debe estarse corriendo el encapsulamiento PPP.

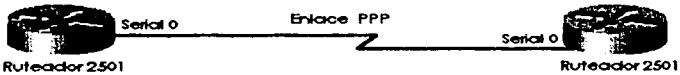
Objetivos de la práctica

Al término de esta práctica, el alumno será capaz de:

- Implementar un enlace utilizando el protocolo puno a punto
- Establecer la autenticación para el acceso controlado

Desarrollo de la práctica

Para esta práctica se usarán 2 ruteadores, con los cuales se establecerá la comunicación de un enlace punto a punto.



En el modo de configuración, nombrar los ruteadores, acceder a la interfase serial y con el comando ayuda, ver que comandos están disponibles, seleccionar PPP como modo de encapsulamiento para las interfases seriales que se van a enlazar encada uno de los dos ruteadores.

Levantar el enlace en cada una de las interfases por medio del comando **no shutdown**, y comprobar que efectivamente exista la comunicación entre los dos ruteadores.

Emitir el comando apropiado para ver el estado del enlace la dirección IP y el protocolo.

A continuación se procederá a demostrar que sucede cuando se establece el enlace PPP con la opción de autenticación en una de las dos interfases seriales de un ruteador y en la otra interfase no.

En el ruteador 1, habilitar la interfase 1 para el encapsulamiento PPP establecer una dirección IP y levantar el enlace y hacer lo mismo para el ruteador 3 en su interfase 0.
Comprobar la comunicación en el enlace y emitir el comando para ver el estado del protocolo y el enlace.

Ahora se establecerá la autenticación CHAP en el ruteador 1 y el ruteador 2, según la interfase que se haya usado para habilitar este enlace.

El procedimiento es el siguiente

En el ruteador 1 se establece la contraseña, la cual nos va a servir para el acceso al ruteador al modo habilitado y además, en este caso, para que el ruteador 1 pueda llevar a cabo la autenticación del ruteador 2 y le permita el ingreso.

Router1(config)#enable secret contraseña

Ahora se le especifica al ruteador el nombre y contraseña del dispositivo que esta en el otro extremo para que se pueda comparar al momento del handshake para que en caso de que coincidan, entonces se le permita el acceso.

Router1(config)#username Nombre **password** contraseña

Teniendo en cuenta lo anterior, estando en la interfase serial 0, se habilita en el protocolo punto a punto la autenticación CHAP, la cual nos va a permitir el acceso al ruteador

```
Router1(config-if)# ppp authentication chap
Router1(config-if)#
```

Nótese que cuando se introduce el comando anterior el enlace se cae, pero cuando se lleva a cabo el procedimiento anterior en el ruteador 2 el enlace se levanta automáticamente.

En el ruteador 2 hay que hacer el mismo procedimiento pero con el **usemame** y la contraseña que se designe para el ruteador 1.

En el ruteador 3 permanecerá sin cambio.

En cada uno de los ruteadores se emitirá el comando para ver el estado del enlace y del protocolo, con el fin de ver su dirección IP asignada

Por último, se verificaran las comunicaciones entre el ruteador 1 y 2 mandando señales de eco, y también entre el ruteador 1 y 3 para notar las diferencias de la autenticación.

Cuestionario

¿En que situación es más comúnmente usado el protocolo punto a punto?

¿Cuáles son las características del protocolo punto a punto?

¿Se puede usar el protocolo punto a punto en una conexión ISDN? Explique

¿Qué diferencias existen entre este protocolo y Frame Relay?

¿En el ejemplo de la práctica, se podrían tener las dos interfases seriales del ruteador 1 activas con la autenticación y el protocolo punto a punto? Explique

Cuestionario preliminar de la práctica 6

De una breve historia del protocolo punto a punto

¿Qué es el protocolo punto a punto?

¿Por qué sólo se puede usar en interfases seriales?

¿Con respecto a que capa del modelo OSI se encuentra el protocolo punto a punto?

¿Por qué es tan común el protocolo punto a punto?

¿Qué es el Handshake y para que sirve?

¿Cuáles son las razones principales por las que se prefiera usar el protocolo punto a punto?

Práctica 7 Frame Relay

- Introducción

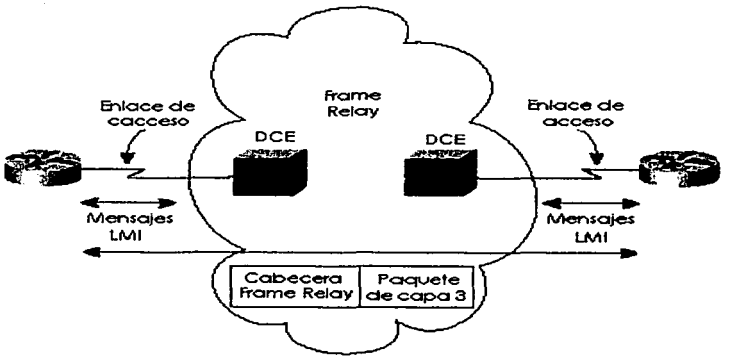
Frame Relay

Frame Relay es un protocolo WAN de alto rendimiento que opera en las capas física y enlace de datos del modelo OSI. Frame Relay originalmente se diseñó para usarse a través de interfases ISDN. Hoy, se usa también sobre una variedad de otras interfases de red.
Frame Relay es un ejemplo de tecnología de conmutación de paquetes. Las redes de conmutación de paquetes permiten a las estaciones del extremo final compartir dinámicamente el medio de red y el ancho de banda disponible.
Se usan paquetes variables de longitud para traslados más eficaces y flexibles. Los cuales se conmutan entre varios segmentos de la red hasta que el destino es alcanzado. Las técnicas de multiplexaje estadístico controlan el acceso de la red en una red de conmutación de paquetes. La ventaja de esta técnica es que acomoda más flexibilidad y el uso más eficaz de ancho de banda.

Protocolos Frame Relay

A diferencia de los enlaces punto a punto, Frame Relay es el protocolo más típicamente usado. Frame Relay es un nombre bien escogido para recordarle que se relaciona más estrechamente a la capa 2 del modelo OSI. El término "Frame" es generalmente asociado con una colección de bits de datos que incluyen una cabecera equivalente de capa 2 de OSI. Por ejemplo, una trama Ethernet incluye la cabecera/remolque. El direccionamiento Frame Relay es más cercano a los estándares de direccionamiento de la capa 2 de OSI y se considera a ser un protocolo de capa 2.

Componentes de Frame Relay



Características de Frame Relay y terminología

Frame Relay es una red multiacceso, la cual, realmente significa que más de dos dispositivos pueden conectarse al medio. El multiacceso es el primer y más obvia diferencia entre Frame Relay y las líneas arrendadas. Sin embargo, se usan las líneas arrendadas como el componente del enlace

de acceso a redes Frame Relay. Considere la figura anterior, la cual es un recurso valioso para repasar los conceptos de Frame Relay.

El enlace de acceso entre el ruteador y el switch Frame Relay, es una línea arrendada. Se conectan ambos sitios representados en la figura hacia algún switch cercano por medio de una línea arrendada. El proveedor de servicio interconecta sus switches para proporcionar la conectividad.

Frame Relay a menudo se describe como una versión aerodinámica de X.25, ofreciendo unas cuantas de las capacidades robustas, tales como el windowing y la retransmisión de datos perdidos que se ofrecen en X.25. Esto es porque Frame Relay opera típicamente sobre instalaciones WAN que ofrecen servicios de conexión más fiables y un grado más alto de fiabilidad que los medios disponibles durante finales de 1970s y principios de los años ochenta que sirvió como plataformas comunes para WANs X.25. Frame Relay es estrictamente un protocolo de capa 2, considerando que X.25 proporciona también los servicios a la capa 3. Esto le permite a Frame Relay ofrecer un desempeño más alto y eficacia de transmisión mayor que X.25 y hace a Frame Relay conveniente para las aplicaciones WAN actuales, tales como la interconexión de LAN.

DLCI (Data Link Connection Identifier)

Los circuitos virtuales Frame Relay son identificados por los DLCIs. Un DLCI (Identificador de Conexión de Enlace de Datos) sirve como esquema de direccionamiento dentro de una red Frame Relay. Los valores DLCI típicamente se asignan por el proveedor de Frame Relay (por ejemplo la compañía de teléfonos). Los DLCIs Frame Relay tienen importancia local, la cual significa que los valores mismos no son únicos en la red Frame Relay WAN. Por ejemplo dos dispositivos DTE conectados por un circuito virtual pueden usar un valor DLCI diferente para referirse a la misma conexión. El proveedor de servicio asigna un DLCI para cada VC que usa Frame Relay para distinguir entre los circuitos virtuales diferentes en la red. Desde que pueden terminarse muchos circuitos virtuales en una interfase multipunto Frame Relay, muchos DLCIs son frecuentemente asociados con él.

Para que se puedan comunicar dispositivos IP en cada extremo de un circuito virtual, su dirección IP necesita ser trazada hacia los DLCIs. Este trazado puede funcionar como un dispositivo multipunto, uno que puede identificar a la red Frame Relay el circuito virtual de destino apropiado para cada paquete que se envía sobre una sola interfase física. Los trazados pueden hacerse dinámicamente con ARP o manualmente con el comando **frame relay map**. Cada DLCI puede tener significado local o global por todas partes dentro de la red Frame Relay. Los DLCIs normalmente son asignados por el proveedor y empiezan con 16.

Configuración Frame Relay

La configuración Frame Relay en un ruteador de Cisco es relativamente fácil si se toman todos los valores predeterminados. Las tablas 1 y 2 resumen los comandos más populares usados para la configuración y verificación de Frame Relay

La parte más difícil de la configuración es determinar cuando y como usar las subinterfases para la configuración de Frame Relay.

Tabla 1 Comandos de configuración Frame Relay

Comando	**Modo de Configuración**	**Propósito**
Encapsulation frame-relay[ietf | cisco]	Interfase	Define el encapsulamiento de Frame Relay que se usa en lugar de HDLC, PPP, y así sucesivamente.
frame-relay lmi-type {ansi | q933a | cisco}	Interfase	Define el tipo de mensajes de LMI enviados al switch.
Bandwidth *num*	Interfase	Envía la velocidad percibida del ruteador de la interfase. El ancho de banda se usa por algunos protocolos de ruteo para influenciar la métrica.
frame-relay map *protocol protocol-address dlci* **[payloadcompress{packet-by-packet | frf9 stac}] [broadcast] [ietf | cisco]**	Interfase	Estáticamente define un mapeo entre una dirección de capa de red y un DLCI.
Keepalive *sec*	Interfase	Define si, y que a menudo se envían los mensajes de pregunta de estado LMI y cuando se esperan.
interface serial *num.sub [pointto-point | multipoint]*	Global	Crea un subinterfase, o hace referencia de una subinterfase previamente creada.
frame-relay interface-dlci *dlci***[ietf | cisco]**	Interfase	Define que un DLCI usado para un VC hacia otro DTE.
frame-relay payload-compress{packet-by-packet | frf9 stac}	Subcomando de la interfase	Define la compresión de la carga útil en las subinterfases de punto a punto

- Conexiones físicas

Los equipos físicos pueden variar entre las organizaciones. Algunas redes pueden usar los ruteadores con CSU/DSUs separados (Unidad de Servicio de Canal / Unidad de Servicio de Datos) y algunos pueden usar ruteadores con CSU/DSUs incorporados. El CSU/DSU se localiza en la locación del cliente de la conexión digital, y se usa para codificar, filtrar, y traducir las comunicaciones hacia y desde la línea digital. En las conexiones Frame Relay, el dispositivo de red que se conecta al switch Frame Relay se conoce como un Dispositivo de Acceso Frame Relay (FRAD - Frame Relay Access Device) también llamado ensamblador/desensamblador Frame Relay. El switch Frame Relay también se llama Dispositivo de Red Frame Relay (FRND - Fame Relay Network Device pronunciado como "friend"). El administrador de la red típicamente maneja la conexión local hasta el punto que entra en el PDN. Las cosas que son parte del PDN, incluyendo el switch Frame Relay, caen bajo el control y la responsabilidad del proveedor de telecomunicaciones. Frame Relay se usa sobre una variedad de interfases de red.

- Circuitos virtuales

Frame Relay puede usarse con casi cualquier interfase serie. Las comunicaciones en una red Frame Relay son orientados a conexión y debe existir un camino de comunicaciones definido entre cada par de dispositivos DTE. Los circuitos virtuales proporcionan un camino de comunicaciones bidireccional desde un dispositivo DTE a otro y se identifican singularmente por un identificador de Conexión de Enlace de Datos (DLCI - Data Link Connection Identifier). La tecnología usada en Frame Relay le permite multiplexar varios flujos de datos sobre el mismo medio físico.

Tabla 3 Conceptos y términos de Frame Relay

Circuito Virtual (VC)	Un VC es un concepto lógico que representa el camino que las tramas viajan entre DTEs. VCs son particularmente útiles al comparar Frame Relay con los circuitos físicos arrendados
Circuito Virtual Permanente	Un PVC es un VC que esta predefinido. Un PVC puede igualarse a una línea arrendada en concepto.
Circuito Virtual Swithceado	Un SVC es un VC que esta configurado dinámicamente. Un SVC puede igualarse a una conexión de dial en concepto.
Equipo Terminal de Datos (DTE)	Los DTEs también son conocidos como equipo de terminación de circuito de datos. Por ejemplo, los ruteadores son DTEs cuando están conectados a un servicio Frame Relay de una compañía de telecomunicaciones.
Enlace de Acceso	El enlace de acceso es la línea arrendada entre un DTE y un DCE.
Proporción de información comprometida (CIR)	El CIR es la tasa a la cual el DTE puede enviar los datos para un VC individual, con el cual, el proveedor se compromete a entregar esa cantidad de datos. El proveedor enviará cualquier exceso de datos de esta tasa para este VC, si su red tiene la capacidad en ese momento. Esta opción afecta típicamente el precio de cada CV.
Tasa de ráfaga	La tasa de ráfaga es la tasa de longitud y tiempo, para el cual, en un VC en particular, el DTE puede enviar más rápidamente que el CIR, y el proveedor está de acuerdo en remitir los datos. Esta opción típicamente afecta el precio de cada VC.
Identificador de conexión de enlace de datos (DLCI)	Un DLCI es una dirección Frame Relay se usa en las cabeceras Frame Relay para identificar el circuito virtual.
Notificación de congestión explícita adelantada (FECN)	El FECN es el bit en la cabecera Frame Relay que señala a cualquiera recibiendo la trama (switches y DTEs) que la congestión está ocurriendo en la misma dirección de la trama. Los switches y DTEs pueden reaccionar retardando la tasa a la cual los datos se envían en esa dirección.
Notificación de congestión explícita retrasada (BECN)	El BECN es el bit en la trama Frame Relay que señala a cualquiera recibiendo la trama (iswitches y DTEs) que la congestión está ocurriendo en la dirección opuesta (hacia atrás) de la trama. Los switches y DTEs pueden reaccionar retardando la tasa por la cual los datos se envían en esa dirección.
Desechar elegibilidad (DE)	El DE es el bit en la cabecera Frame Relay que señala hacia un switch para saber, si las tramas deben ser desechadas, por favor escoja esta trama para desechar en lugar de otra trama sin el bit DE puesto.
Multiacceso de monobroadcast (NBMA)	NBMA se refiere a una red en la cual las transmisiones no son soportadas, pero más dedos dispositivos pueden conectarse.
Interfase de Dirección local (LMI)	LMI es el protocolo usado entre un DCE y DTE para manejar la conexión. Los mensajes de la señalización para SVCs, mensajes de estado PVC, y keepalives son todos mensajes LMI.
Procedimiento de acceso al enlace, servicio portador modo trama (LAPF)	LAPF es la cabecera y trailer básica de Frame Relay; incluye DLCI, FECN, BECN, y bits DE.

Frame Relay separa cada flujo de datos en lógico (mantenimiento de software) las conexiones llamadas circuitos virtuales las cuales llevan los datos transferidos en la conexión entre dos dispositivos DTE. Dos tipos de circuitos virtuales, SVCs (Circuito Virtual Conmutado) y PVCs (Circuito Virtual Permanente) conectan los puertos Frame Relay. Los Circuitos Virtuales conmutados (SVCs) permiten el acceso a través de una red Frame Relay, estableciendo un camino hacia los puntos

finales, solo cuando la necesidad se incrementa y dando de baja el camino cuando ya no se necesita. Los Circuitos Virtuales permanentes (PVCs) son conexiones establecidas que se usan para la transferencia de datos frecuentes y consistentes entre los dispositivos DTE de la red Frame Relay. Los SVCs y PVCs pueden coexistir en los mismos sitios y ruteadores. Por ejemplo, los ruteadores en las oficinas remotas podrían establecer PVCs a la oficina principal central para las comunicaciones mas frecuentes, pero establecer entre sí SVCs como sea necesario para la comunicación intermitente.

Desarrollo de la práctica

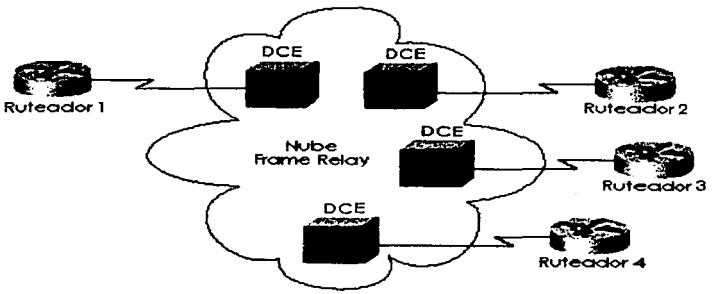
Objetivos:

Al término de la práctica el alumno será capaz de:

- Establecer un enlace Frame Relay entre dos ruteadores
- Configurar una red Frame Relay de cuatro ruteadores totalmente interconectada

Para esta práctica, se debe cargar en el simulador la topología Frame Relay predeterminada, la cual consta de 8 ruteadores conectados por medio de su interfase serial hacia una nube Frame Relay. Se van a utilizar 4 ruteadores para lograr la conectividad entre el ruteador 1 y los otros tres.

Lo primero para realizar el enlace, es darle un nombre al ruteador 1 y configurar la interfase serial 0, establecer el encapsulamiento Frame Relay y dar de alta la interfase. Nótese que la interfase al darse de alta, después de unos segundos automáticamente se da de baja. La interfase se restablecerá cuando se haya completado un enlace en el otro ruteador.



Ahora lo siguiente es configurar las subinterfases, o sea que la interfase serial 0 se va a segmentar en varios canales de comunicación, los cuales va a tener una dirección IP y un DLCI para que el switch del proveedor de servicio Frame Relay pueda entregarlo al DLCI correcto en el otro extremo

```
UNAM(config-if)#exit
UNAM(config)#
UNAM(config)#interface serial 0.100
```

```
UNAM(config-subif)# ?
arp               set arp type (arpa, probe, snap) or timeout
bandwidth         set bandwidth informational parameter
cdp               cdp interface subcommands
description       interface specific description
encapsulation
exit              exit from interface configuration commands
frame-relay       set frame relay parameters
ip                interface internet protocol config commands
ipx               Novell/IPX interface subcommands
map-group         configure static map group
mtu               configure NTP
shutdown          shutdown the selected interfaces

UNAM(config-subif)#frame-relay interface-dlci 102
UNAM(config-subif)#
UNAM(config-subif)#ip add 172.16.1.1 255.255.255.0
```

Hasta este punto, la subinterfase para el ruteador 2 ya ha sido cread, ahora se procederá con las demás interfases del mismo modo, solamente que se cambiará el número de subinterfase, el número de DLCI y su dirección IP

```
UNAM(config-if)#exit
UNAM(config)#interface serial 0.200
UNAM(config-subif)#frame-relay interface-dlci 103
UNAM(config-subif)#ip add 172.16.2.1 255.255.255.0
UNAM(config-if)#exit
UNAM(config)#
```

Ya que se ha terminado de configurar las subinterfases en el ruteador 1, se procede a configurar la interfase en los demás ruteadores.
Para los demás ruteadores no se tienen que configurar subinterfases, ya que los ruteadores 2, 3 y 4 solo tienen conexión hacia el ruteador 1.

```
Aragón(config)#
Aragón(config)#interface serial 0
Aragón(config-if)#encapsulation frame-relay
Aragón(config-if)#no shutdown
Aragón(config-if)#frame-relay interface-dlci 201
%LINK-3-UPDOWN: Interface serial 0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on interface serial 0, changed state to up
21:49:39 %FR-5-DLCICHANGE: Interface serial0 - DLCI 201 state changed to ACTIVE
Aragón(config-if)#ip add 1772.16.1.2 255.255.255.0
Aragón(config-if)#
```

Nótese que cuando se estableció el número de DLCI, el enlace se levantó automáticamente, anunciando el cambio de estado del DLCI

Tabla 1

Ruteador	Interfase	Subinterfase	Dirección IP	DLCI
UNAM				
Aragón				
Iztacala				
Acatlan				

Cuestionario:

De una explicación de cómo se llevo a cabo la numeración de los DLCI

¿Hasta cuantas subinterfases se pueden tener en una interfase serial?

¿Es conveniente diseñar una red Frame Relay como la anterior? Explique

¿Qué es lo que compone la nube Frame Relay?

Implemente una red Frame Relay Totalmente comunicada entre todos los ruteadores y elabore un reporte con los detalles

Cuestionario preliminar de la práctica 8

¿Qué significa Frame Relay?

¿Qué diferencia existe entre Frame Relay y X.25?

¿Qué son los PVC y SVC?

¿Qué es el DLCI?

¿Qué capas del modelo OSI usa Frame Relay?

¿Qué es un DCE y un DTE?

¿Cuál es la velocidad máxima de transferencia de datos que se alcanza en la actualidad con Frame Relay?

¿Qué significa VoFR? Y de un ejemplo

Práctica 8 ISDN

- Introducción

Uso típico de ISDN

ISDN se usa típicamente para las conexiones de marcación de discado temporal. El costo atractivo también ha causado que algunas compañías usen permanentemente conexiones ISDN, en lugar de las líneas arrendadas. Las líneas ISDN pueden proporcionar el acceso a 128 Kbps, usando ambos canales B. La compresión puede aumentar el rendimiento, obteniendo potencialmente 500 Kbps de rendimiento a través de la línea.

Las conexiones temporales entre los ruteadores es otro uso típico de ISDN, ambos para el respaldo y para la conexión ocasional. Las conexiones ocasionales incluirían el tráfico para los sitios que no usan aplicaciones en línea o vídeo conferencia, y casos en los cuales se desea un ancho de banda adicional entre los sitios. La mayoría de las configuraciones necesarias para estas conexiones ocasionales se relaciona a un tema llamado ruteo de marcación bajo demanda (dial-on-demand routing - DDR)

Los escenarios en la figura 1 pueden describirse de la manera siguiente:

- Caso 1 muestra el ruteo de marcación bajo demanda. La lógica se configura en los ruteadores para disparar la marcación de discado cuando el tráfico que necesita llegar a otro sitio es enviado por el usuario.
- Caso 2 muestra un ambiente del telecommuting típico.
- Caso 3 muestra la típica topología de marcación de discado de respaldo. La línea arrendada falla, así que una llamada ISDN se establece entre los mismos dos ruteadores.
- Caso 4 muestra un caso en que un ISDN BRI podría ser usado para marcar directamente hacia otro ruteador para reemplazar un enlace de acceso Frame Relay o un VC fallido.
- Caso 5 describe una línea ISDN que podría usarse para marcar en la red Frame Relay del proveedor, reemplazando un VC fallido o enlace de acceso con un VC corriendo sobre una conexión ISDN hacia el switch Frame Relay.

- Ruteo bajo demanda y configuración ISDN

DDR define la lógica detrás de cuando un ruteador escoge marcar otro sitio, si se usa ISDN, serial síncrona, o si se usan interfases seriales asíncronas.: la lógica de DDR es la misma para cualquiera de los tres tipos de interfases de marcación. DDR incluye unas variaciones: la variación llamada "DDR legacy" se cubre en este capítulo.

Figura 1 Conexiones Ocasionales Típicas Entre los Ruteadores

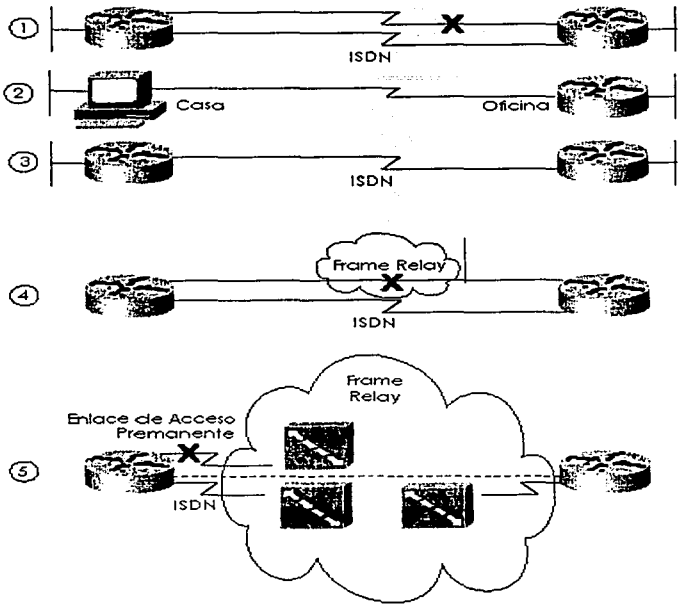


Tabla 8-30 Comandos de Configuración ISDN

Comando	Modo de configuración	**Propósito**
isdn switch-type *switch-type*	Global o Interfase	Define al ruteador el tipo de switch ISDN el cual la línea ISDN se conecta en la oficina central.
isdn spid1 *spid.*	Interfase	Define el primer SPID
isdn spid2 *spid.*	Interfase	Define el segundo SPID
isdn caller *number*	Interfase	Define un número válido para las llamadas entrantes al usar la proyección de llamada.
isdn answer1 [*called-party-number*][:*subaddress*]	Interfase	Especifica el número ISDN o subdirección que debe usarse en las llamadas entrantes para que este ruteador conteste.
isdn answer2 [*called-party-number*][:*subaddress*]	Interfase	Especifica un segundo número ISDN o subdirección que debe usarse en las llamadas entrantes para que este ruteador conteste.
dialer-list [*list nnn*] **protocol**[*protocol-type*] **permit** | **deny**	Global	Define el tipo de tráfico considerado interesante.

dialer-group *n*	Interfase	Habilita la lista de marcaje en esta interfase.
dialer in-band	Interfase	Habilita la marcación dentro en esta interfase. Este comando sólo se usa para líneas seriales que se conectan hacia un TA, no para interfases ISDN nativas que usan el canal D fuera de banda.
dialer string *string*	Interfase	Es el cordón del marcación usado al marcar un sólo sitio.
dialer map *protocol next-hop address* [name *hostname*] [speed *56 | 64*][broadcast] *dial-string*	Interfase	Es el cordón de marcación para alcanzar el siguiente salto. Sin embargo, el comando map se usa al marcar más de un sitio. Este también es el nombre usado para la autenticación. La transmisión se asegura que las copias de transmisiones vayan hacia esta dirección del siguiente salto.

Tabla 8-31 Comandos EXEC ISDN relacionados

Comando	Función
show interfaces bri *number*[*:b-channel*]	Incluye la referencia hacia las listas de acceso habilitadas en la interfase.
show controllers bri *number*	Muestra las estadísticas y el estado de la capa 1 para los canales B y D.
show isdn {active | history | memory | status | timers}	Muestra información variada de estado ISDN.
show interfaces bri *number*[[*:bchannel*] *| [first] [last]*] **[accounting]**	Despliega la información de la interfase acerca del canal D o los canales B.
show dialer interface bri *number*	Lista los parámetros DDR en la interfase BRI. Muestra si actualmente se ha marcado, indicando el estado actual. También muestra intentos previos para marcar y si tuvieron éxito.
debug isdn q921	Listas los mensajes ISDN de la capa 2.
debug isdn q931	Lista los mensajes ISDN de la capa 3 (llamados setup/teardown).
debug dialer {events | packets}	Lista la información cuando un paquete se dirige fuera de una interfase de marcación, diciendo si el paquete es interesante.

Desarrollo de la práctica

Objetivo:

- Entenderá el funcionamiento de ISDN
- El alumno será capaz de configurar un enlace ISDN entre dos ruteadores

Para esta práctica se usarán los ruteadores 1 y 2 de la topología predefinida, ya que es la que cuenta con una conexión ISDN

Lo primero que se necesita es establecer una dirección IP en cada una de las interfases BRI del ruteador, no olvidando darla de alta
Ahora nos enfocaremos a la configuración ISDN. El simulador tiene la capacidad de imitar el comportamiento de la línea, por lo que debemos especificar el tipo de switch ISDN que se esta usando por medio de los comandos **Isdn switch-type**. En esta parte se tienen las siguientes opciones:

```
Router(config)#isdn switch-type ?

basic-1tr6          1TR6 switch type for Germany
basic-5ess          AT&T 5ESS switch type for the U.S.
basic-dms100        Nothern DMS - 100 switch type
basic-net3          NET3 switch type for U K and Europe
basic-ni            National ISDN switch type
basic-ts013         TS013 switch type for Australia
ntt                 NTT switch type for Japan
vn3                 VN3 and VN4 switch types for France
```

El modelo de switch que se elegirá será el predefinido o sea el switch **basic-ni**

Ahora lo hay que especificar el SPID o Service Profile Identifier, el cual es un número que proporciona el proveedor de servicio de Internet, para identificar la configuración de la línea del servicio ISDN básico. Cada SPID apunta hacia la configuración de la línea y la información de la configuración en el switch ISDN del proveedor de servicio de Internet.
En este caso elegiremos **spid 1** con el número predefinido 32177820010100 solamente para el ruteador 1.

Nota Cabe mencionar que se puede cambiar el modelo de switch y de spid cuando se configura una topología de red nueva en la opción del simulador de diseño de red propia, esto quiere decir que cuando se configure la conexión ISDN se puede hacer una elección de los modelos de switch anteriores y el número de spid puede ser elegido arbitrariamente.

En este punto, debemos tener ya comunicación con el switch del proveedor de servicio, y para probar lo anterior, se puede verificar emitiendo el comando **show isdn status** el cual va a dar como resultado lo siguiente:

```
Router#show isdn status
Global ISDN Switchtype = basic-ni
ISDN BRI0 interface
        dsl 0, interface ISDN switchtype = basic-ni
Layer 1 Status:
        ACTIVE
Layer 2 Status:
        TEI = 64, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
        TEI 64, ces = 1 state 8(established)
        Spid 1 configured, no LDN, spid 1 sent, spid 1 valid
Layer 3 Status:
        0 Active Layer 3 Call(s)
        Active Dsl 0 CCBs = 0
        The Free Channel Mask 0x80000003
        Number of L2 Discards = 0, L2 Session ID = 100
        Total Allocated ISDN CCBs = 0
```

Aquí se muestra la información del estado de las capas 1, 2 y 3. Se puede apreciar que la capa 1 ya se encuentra activa

Ahora debemos especificar el número telefónico el cual se va a marcar cuando se requiera que el enlace se active. En la interfase BRI 0 se tiene que seleccionar los comandos **dialer strig**, usando el número de teléfono predeterminado en la conexión ISDN, o sea 7782001

Ya que ISDN cuesta dinero cuando la conexión se establece, lo que se desea es tener la conexión activa solo cuando está en uso. Para ello se usan los grupos de marcación y las listas de marcación. Una lista de marcación es una lista que permite o niega el tráfico. Esto significa que nosotros debemos especificar una lista de marcación de los "protocolos ip permitidos" lo que significa que cualquier tráfico IP será permitido. Para configurar una lista de marcación, se debe hacer lo siguiente:

```
Router(config)#dialer-list1 protocol ip permit
```

Ahora que se ha configurado la lista de marcaje, se debe asociar esa lista a una interfase, por lo que se configurará un grupo de marcaje en la interfase:

```
Router(config-if)#dialer-group 1
```

Ahora solo resta hacer el mismo procedimiento pero en el ruteador 2 en la interfase BRI 0,

Nombrara al ruteador y establecer una dirección IP en la interfase BRI 0, no olvidando darla de alta.

Indicarle al ruteador que tipo de switch es el que la compañía de teléfonos tiene, ya que es al que nos vamos a conectar

En la interfase BRI 0 hay que establecer el SPID el cual va a ser el número predefinido 32177820020100

Establecer el número telefónico al que se debe marcar en desde el ruteador 2, el cual va a ser el número predefinido 7782002

Después, crear la lista de marcaje en el modo global del ruteador par que todo el tráfico del protocolo IP sea permitido en el otro ruteador

Y por último se asocia el grupo de marcaje a la interfase usando el comando **dialer group**

Cuestionario:

¿Cuál es el uso principal que se le da a un enlace ISDN conectado al ruteador?

¿Sería conveniente basar la red en enlaces ISDN?

Configure una red LAN conectada a un ruteador con un enlace ISDN hacia un ruteador con otra red LAN y compruebe la comunicación entre todos los dispositivos. Entregue un resumen del procedimiento

¿A que grupo funcional y a que punto de referencia pertenece un ruteador conectado a la ISDN?

Si se tuviera la oportunidad de diseñar una red corporativa en varios estados de la república Mexicana, ¿que sería lo mas conveniente usar, enlaces punto a punto Frame Relay o ISDN? Explique.

Cuestionario preliminar de la práctica 8:

¿Qué es la ISDN?

¿Cuál es la diferencia entre ISDN los enlaces punto a punto?

¿Explique cuál es la diferencia del servicio ISDN en norte América y Europa?

¿Cuál es la serie de estándares que definen la ISDN?

Diga que y cuales son los puntos de referencia y grupos funcionales de ISDN

Conclusiones

En nuestro país, hoy en día las especializaciones se están volviendo cada vez más indispensables, en cualquier área laboral. El área de las comunicaciones, siendo tan amplia, ofrece la oportunidad de especializarse a fondo en sus diferentes ramas, una de estas ramas, es la que comprende a las redes de datos. Estas especializaciones o "Certificaciones", otorgan una validez en cuanto a conocimientos que se requieren para desempeñar cierto tipo de trabajo especializado. Las certificaciones las expide una empresa privada externa a una institución educativa y garantiza el dominio de ciertas habilidades que posee la persona certificada.

Cisco Systems es una empresa Estadounidense líder en la fabricación de ruteadores y switches, con base en San José California. Cisco está interesada en que haya gente capaz de implementar sus soluciones de telecomunicaciones en el mercado, para incentivar esto, aplica un examen de certificación en base a sus habilidades de configuración, diseño y soporte técnico, de sus equipos. Esto tiene un valor agregado para el currículum personal, resultando en una mejor remuneración.

El propósito de esta práctica es dar a los alumnos de Ingeniería de comunicaciones, una primera visión del comportamiento de los dispositivos de interconexión de redes y a su vez profundizar en los temas que son necesarios para comprender y si se desea tomar el examen de certificación con un poco mas de conocimiento e investigación propia.

Las prácticas están elaboradas para que el alumno comience desde la comprensión de cómo funcionan los ruteadores y switches de Cisco, hasta la configuración básica de ISDN, con toda la información teórica que se requiere. La práctica tiene que ser complementada con información adicional que debe ser proporcionada por el instructor del laboratorio, el cual puede referirse a esta tesis como apoyo. Además, el simulador que se propone en esta tesis, permite que el instructor pueda desarrollar sus habilidades e implementar prácticas adicionales o sugerir cambios en las prácticas de a cuerdo como se presenten las necesidades de configuración en el futuro.

La falta de un laboratorio de comunicaciones especificamente y de conocimiento de lo que es la certificación Cisco CCNA, fue el motivo principal para esta investigación, ya que otras instituciones educativas, brindan la oportunidad a sus alumnos de llevar un laboratorio supervisado por Cisco, y al final de sus estudios estar preparado para tomar el examen de certificación. Por lo cual, usted se podrá imaginar la enorme desventaja que enfrentamos los egresados de la UNAM.

Si bien esta serie de prácticas es introductoria a lo que se puede llegar a ver en un curso de Cisco, es lo suficiente para que el alumno puede decidir si esa área es la que real mente le interesa, y si es así, entonces al término de sus estudios tenga cierto conocimiento de lo que es el soporte técnico, diseño e implementación de las redes de datos y recientemente, redes de datos con aplicaciones de voz (Voz sobre Frame Relay y Telefonía IP)

Para la mayoría de las empresas (desafortunadamente), se le da mayor prioridad a una persona certificada en Cisco, que a un recién egresado y titulado de esta área, por eso la importancia de que se tenga un conocimiento básico de cono es la configuración de los equipos de interconexión de redes de datos, hasta que se logre implementar este laboratorio por Cisco Systems.

Bibliografía

- WENDELL ODOM
  Cisco CCNA Exam #640-507 Certification Guide
  201 West 103rd Street, Indianapolis, IN 46290 USA
  Cisco Press

- GEORGE C. SACKETT
  Manual de outers Cisco
  Madrid, Edificio Valrealty, 1a planta Basauri,
  Mc Graw-Hill Osbourne Media