TÉCNICAS PARA LA GESTIÓN DEL ANCHO DE BANDA EN LA WAN CON SOPORTE EN ROUTERS CISCO 2600

GUSTAVO ADOLFO AGUDELO FRÍAS

FERNANDO DE ORO BARRIOS

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE SISTEMAS

CARTAGENA DE INDIAS D.T. y C.

2004

TÉCNICAS PARA LA GESTIÓN DEL ANCHO DE BANDA EN LA WAN CON SOPORTE EN ROUTERS CISCO 2600

GUSTAVO ADOLFO AGUDELO FRÍAS

FERNANDO DE ORO BARRIOS

Monografía presentada como requisito para optar

al título de Ingeniero de Sistemas

Director

ISAAC ZÚÑIGA SILGADO

Ingeniero de Sistemas

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE SISTEMAS

CARTAGENA DE INDIAS D.T. y C.

2004

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

ARTICULO 107

La institución se reserva el derecho de propiedad intelectual de todos los trabajos de grupo aprobados, los cuales no pueden ser explotados comercialmente sin su autorización. Esta observación debe quedar impresa en parte visible del proyecto.

Cartagena de Indias, D.T. y C., 24 de junio de 2004

Señores:

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR.

COMITÉ DE EVALUACIÓN DE PROYECTOS.

ESCUELA DE INGENIERÍAS.

Ciudad.

Reciban un cordial saludo.

Por medio de la presente me permito informarles que he llevado a cabo la dirección de la monografía de los estudiantes GUSTAVO ADOLFO AGUDELO FRÍAS y FERNANDO DE ORO BARRIOS, titulada "TÉCNICAS PARA LA GESTIÓN DEL ANCHO DE BANDA EN LA WAN CON SOPORTE EN ROUTERS CISCO 2600".

Cordialmente,

_____

ISAAC ZÚÑIGA SILGADO

Ingeniero de Sistemas

Cartagena de Indias, D.T. y C., 24 de junio de 2004

Señores:

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR.

COMITÉ DE EVALUACIÓN DE PROYECTOS.

ESCUELA DE INGENIERÍAS.

Ciudad.

Reciban un cordial saludo.

Por medio de la presente les presentamos para evaluación y aprobación la monografía titulada "TÉCNICAS PARA LA GESTIÓN DEL ANCHO DE BANDA EN LA WAN CON SOPORTE EN ROUTERS CISCO 2600", desarrollado por GUSTAVO ADOLFO AGUDELO FRÍAS y FERNANDO DE ORO BARRIOS.

Esperamos que esta monografía cumpla con las expectativas y requisitos planteados por la Institución.

Atentamente,

GUSTAVO ADOLFO AGUDELO FRÍAS

FERNANDO DE ORO BARRIOS

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Cliente: Cualquier estación de trabajo en una red que solicita servicios a un servidor de cualquier naturaleza.

Estación de trabajo: Cualquier computador conectado a la red. Antiguamente sólo se llamaba estación de trabajo a los ordenadores más potentes, en la actualidad no es así. Todas las estaciones de trabajo deben incorporar su tarjeta de red.

Nodo: Cualquier estación de trabajo, terminal, computador personal, impresora o cualquier otro dispositivo conectado a la red.

Servidor: Se trata de una estación de trabajo que gestiona algún tipo de dispositivo de la red, como pueden ser impresoras, fax, **modems**, discos duros, etc., dando servicio al resto de las estaciones, no siendo necesario que dichos dispositivos estén conectados de forma directa a esta estación.

Medio de transmisión: Se trata de cualquier medio físico, incluso el aire, que pueda transportar información en forma de señales electromagnéticas. El medio de transmisión es el soporte de toda la red.

Método de acceso al medio: Se podrían citar como medios más comunes el paso de testigo, acceso múltiple por detección de portadora con y sin detección de colisiones, **polling**, contención simple, etc. Los métodos de control de acceso al medio se encuentran dentro del nivel de enlace del modelo OSI, por lo que en realidad pueden entenderse como protocolos de red.

Protocolos de red: Definen las diferentes reglas y normas que rigen el intercambio de información entre nodos de la red. Los protocolos establecen reglas a muchos niveles: desde cómo acceder al medio, hasta cómo encaminar información desde el origen hasta su destino, pasando por la descripción de las normas de funcionamiento de todos y cada uno de los niveles del modelo OSI de la ISO.

Paquete: Es básicamente el conjunto de información a transmitir entre dos nodos. Cuando una aplicación quiera enviar información a otra aplicación en otro nodo, lo que hace es empaquetar dicha información, añadiendo datos de control como la dirección de la máquina que envía la información (dirección origen) y la dirección de la máquina a la que va destinada la información (dirección destino).

Concentradores (**Hubs**): Dispositivo que centraliza la conexión de los cables procedentes de las estaciones de trabajo. Existen dos tipos de concentradores: pasivos y activos.

Puentes (**Bridges**): Nos permiten dos cosas: primero, conectar dos o más redes entre sí, aun teniendo diferentes topologías, pero asumiendo que utilizan el mismo protocolo de red, y segundo, segmentar una red en otras menores. Los puentes trabajan en el nivel de enlace del modelo OSI de la ISO.

Enrutadores (**Routers**): Se trata de dispositivos que interconectan redes a nivel de red del modelo OSI de la ISO. Realizan funciones de control de tráfico y enrutamiento de paquetes por el camino más eficiente en cada momento.

Pasarelas (**Gateways**): Se trata de dispositivos que trabajan a nivel de aplicación del modelo OSI de la ISO. Es el más potente de todos los dispositivos de interconexión de red. Nos permiten interconectar redes de diferentes arquitecturas, es decir, de diferentes topologías y protocolos.

Ancho de banda (**bandwidth**): Es la capacidad de transporte de información de un canal de comunicación. El canal puede ser análogo o digital. Las transmisiones análogas como las llamadas por teléfono, radio AM y FM, y la televisión son medidas en ciclos por segundos (hertz o Hz). Las transmisiones digitales son medidas en **bits** por segundo. Para sistemas digitales, el termino “ancho de banda” y “capacidad” usualmente son intercambiables, y las capacidades de transmisión actual se indican como la tasa de transferencia de datos.

RESUMEN

Se presenta una recopilación de las técnicas para la gestión del ancho de banda en la WAN, agrupadas según el enfoque que utilizan para resolver el problema de desempeño de la red. La inclusión dentro de una agrupación no es estricta lo que implica que una técnica puede estar involucrada en varias agrupaciones.

Luego se estudian y documentan las capacidades de la familia de **routers** Cisco 2600 para soportar protocolos WAN (ATM, Frame Relay, RDSI, SMDS y X.25).

Se muestra en forma detallada cómo simular o emular una implementación completa del protocolo Frame Relay y la técnica de gestión del ancho de banda **Frame Relay Traffic Shaping**, en los **routers** y **routers** que actúan como **switches** Frame Relay, al configurar las dos interfases seriales con que actualmente disponen los **routers** del laboratorio de redes de la Universidad Tecnológica de Bolívar.

Al final se encuentran las conclusiones del por qué se realizaron las prácticas de laboratorio utilizando Frame Relay y notas acerca de la recopilación de las técnicas de gestión del ancho de banda en la WAN.

INTRODUCCIÓN

Se quiere prestar atención con este trabajo en las capacidades que brindan los **routers** Cisco 2600, con que cuenta la UTB, para simular una tecnología WAN de la forma más completa posible; esto es, realizando la configuración del lado del usuario y las configuraciones de las interconexiones de los dispositivos de red del proveedor de servicios (**carrier**) para brindar el servicio de determinado protocolo WAN. Lo anterior atado a las capacidades de los **routers** con que cuenta el laboratorio de redes, limitado al uso de dos interfases seriales por **router**.

Además se presenta una recopilación lo más extensa posible de las técnicas de gestión del ancho de banda en la WAN que se utilizan o han utilizado; de antemano se previene al lector que no están todas las que son o son todas las que están. Debido a la gran cantidad de trabajo que han realizado en este campo los fabricantes de dispositivos de redes y los organismos encargados de la estandarización de las telecomunicaciones. También porque una misma técnica puede ser llamada de varias formas por distintos fabricantes para sus fines particulares o porque algunas técnicas han pasado de ser propietarias a estandarizadas o viceversa.

OBJETIVOS

- Brindar los conceptos básicos sobre los protocolos WAN que soporta la familia de **routers** Cisco 2600 que tiene a su disposición la Universidad Tecnológica de Bolívar.

- Configurar los **routers** de forma que simulen el comportamiento de las interconexiones internas de un proveedor de servicios, para los protocolos WAN: RDSI/ISDN, Frame Relay y ATM.

- Configurar los **routers** de forma que se pueda establecer una comunicación entre dos usuarios en extremos opuestos de la “nube” del proveedor, para los protocolos seleccionados.

- Mostrar paso a paso las actividades con los **routers** de forma que la persona pueda aprender y mecanizar una secuencia adecuada de pasos para configurar los protocolos WAN escogidos.

- Recopilar y documentar las técnicas utilizadas para mejorar la gestión del ancho de banda en la WAN.

- Recopilar y documentar las técnicas utilizadas para implementar la calidad de servicio (QoS) en la WAN.

1 SITUACIÓN ACTUAL DEL MUNDO DE LAS TELECOMUNICACIONES

Las redes de telecomunicaciones actuales están caracterizadas por la especialización. Esto quiere decir que para cada servicio individual de telecomunicación, existe al menos una red para transportar este servicio. A continuación se describen algunos ejemplos de redes públicas existentes[1]:

- La red de **Telex** transporta sólo información de **Telex**, esto es, mensajes de caracteres a muy baja velocidad (300 bits/s). Los caracteres son codificados en un código específico de 5 bits, el código de Baudot.

- El servicio Telefónico Convencional (**Plain Old Telephone Service**, POTS) es transportado vía red conmutada de telefonía pública (**Public Switched Telephone Network**, PSTN). Esta red, ofrece a los clientes los servicios típicos de voz.

- Los servicios de datos son transportados también en la red pública ya sea

1 FLORES PÉREZ, Guido Fidel. Características de los Equipos ATM y su respuesta ante Tráfico Multimedia. Méjico. 1996

por medio de la Red de Datos de Conmutación de Paquetes (**Packet Switched Data Network**) basada en protocolos X.25, o como se realiza en un número muy limitado de países, por medio de una Red de Datos de Conmutación de Circuitos (**Circuit Switched Data Network**) basada en el protocolo X.21.

- Las señales de Televisión pueden ser transportadas en tres formas: Radiodifusión (**Broadcast**) vía ondas de radio usando una antena terrestre, por la red de distribución de cable coaxial (CATV o Cable-TV) o como se ha hecho últimamente, vía satélite, usando el llamado Sistema de Difusión Directa (**Direct Broadcast System**).

- En el dominio privado, los servicios de datos son transportados principalmente por una red de área local (LAN). Las más famosas son Ethernet, Token bus y Token ring (series IEEE 802).

Cada una de estas redes fue diseñada específicamente para ese servicio y usualmente no se utiliza para transportar un servicio diferente. Por ejemplo, la red original de CATV no permite el transporte de POTS; o la PSTN no transporta señales de TV; o la transferencia de voz sobre una red X.25 es muy problemática debido al retardo tan largo existente en la comunicación punto a punto, además del **jitter** existente en este retardo.

Sólo en casos limitados y especiales pueden algunos tipos de red dar servicio a otros diferentes para los que originalmente fueron diseñados. Este es el caso de la red telefónica conmutada, que puede llevar servicios de datos a una velocidad moderada si se instalan **modems** en los dos extremos a comunicar.

Una consecuencia importante de esta especialización de las redes es la frecuente existencia de un número muy grande de redes independientes a nivel mundial, cada una requiriendo sus fases de diseño, operación y mantenimiento. Adicionalmente, el dimensionamiento de cada red debe hacerse para cada tipo de servicio individualmente. Aunque los recursos estén disponibles libremente en una red, estos no pueden ser usados por un tipo de servicio diferente. Por ejemplo las horas pico de la red telefónica son de 9 AM a 5 PM mientras que las de la red CATV son durante la tarde y noche. Puesto que cada una de estas redes cuenta con una infraestructura por separado es imposible compartir los recursos y de esta manera balancear y aprovechar mejor su capacidad ya que cada una de estas redes se debe dimensionar en función de la máxima carga a utilizar aunque tenga tiempos con carga muy baja.

Un primer paso, hacia una sola red universal, fue la introducción de la N-ISDN (**Narrow Integrated Services Digital Network** o RDSI-BE Red Digital de Servicios Integrados de Banda Estrecha) sobre la cual la voz y datos son

transportados sobre un sólo medio. Esta red no puede transmitir señales de TV debido a sus capacidades limitadas de ancho de banda, por lo tanto, aún se requiere de una red especial para TV. Aún en N-ISDN la integración de servicios de banda estrecha tales como la voz y los datos puede considerarse como algo ciertamente limitado a pesar de que el acceso del usuario a la red está totalmente integrado tanto en la interfaz de acceso por régimen básico (BRI) como en la de régimen primario (PRI). Sin embargo, dentro de la misma red, existirá todavía por un buen tiempo una subred de conmutación de paquetes y una de conmutación de circuitos como dos redes sobrepuestas incapaces de transportar otros tipos de tráfico y cada una dimensionada ya sea para voz o para datos X.25. Con la definición de la arquitectura B-ISDN (RDSI de Banda Ancha), se han tenido en cuenta todos los servicios posibles, tanto presentes como futuros.

Como ejemplos típicos de servicios contemplados, denominados genéricamente como servicios “Multimedia” o de “Banda Ancha”, figuran:

- Servicios de Comunicación Interactiva

  Vídeo-conferencia.

  Multi-vídeo conferencia.

  Servicios de Trabajo Cooperativo (**Computer Supported Cooperative Work**, CSCW).

- Servicios de Recuperación de Información.

Acceso a Bases de Datos Multimedia (incluidos los servicios en formato hipermedia como, actualmente los correspondientes al WWW).

Vídeo Distribución (**Video Retrieval**) y Vídeo bajo demanda (**Video on Demand**).

Mensajería Multimedia.

- Servicios de Distribución

  Servicios de Distribución de TV de Alta Calidad

- Servicios de Transmisión de Datos de Alta Velocidad.

  Servicios de Interconexión de Redes de Área Local.

En definitiva las redes de hoy son muy especializadas y sufren de un gran número de desventajas, siendo las más importantes:

- Dependencia del Servicio
- Inflexibilidad
- Ineficiencia

Tomando en cuenta todas estas consideraciones en flexibilidad, dependencia del servicio y utilización de los recursos, es muy importante que sólo exista una red y que esta red del futuro sea independiente del servicio que preste.

2 GESTIÓN DEL ANCHO DE BANDA EN LA WAN

La gestión del ancho de banda (**Bandwidth Management**) también conocida como gestión del tráfico (**Traffic Management**), trata de asegurar que suficiente ancho de banda esté disponible para cumplir con las necesidades del tráfico, y si no, gestionar el tráfico en una forma que asegure que el tráfico crucial pase. Hay varios tópicos que tratan de cómo gestionar el ancho de banda.

Por ser los tópicos tan extensos para ser abordados en el contexto de este documento monográfico, a continuación se presenta un resumen de los grupos más importantes de técnicas y se invita al lector interesado en conocer con más detalles los integrantes de cada grupo, a revisar el documento complementario que se encuentra en el CD-ROM adjunto.

2.1 CALIDAD DE SERVICIO (QOS)

A continuación se presenta un panorama general de la QoS, visto desde una perspectiva temporal localizada en el año 1998, realizada por Eric Hindin en su artículo titulado “Say what? QoS in English”. Las diferencias de hoy con respecto

al desarrollo de las ideas no son abismales; pero el desarrollo y estandarización en los protocolos si está muy avanzado hoy día.

QoS es una forma de asignar recursos en **routers** y **switches** para que los datos lleguen a su destino de una forma rápida, consistente y confiable. A medida que las aplicaciones incrementan su demanda por ancho de banda y retrasos bajos, la QoS se está convirtiendo en un alto criterio de compra por parte de los compradores de **hardware** de redes y una forma clave de los vendedores de diferenciar sus productos.

Hay pocas maneras de proveer QoS en las redes. El método más simple es otorgarle más ancho de banda donde hay problema, lo cual se conoce como **overengineering** la red. La QoS también se puede proveer usando características y capacidades como priorización de datos (**data priorization**), colas (**queuing**), evitar la congestión (**congestion avoidance**) y modelado el tráfico (**traffic shaping**). Las redes basadas en políticas (**policy-based networks**) unirán todas estas características en un solo sistema automatizado que asegure la QoS de extremo a extremo.

Overengineering es la manera más simple de asegurar QoS en la

LAN. La presión de la competencia, los nuevos procesos en la fabricación de **chips** que permiten que un gran número de funciones sean integradas dentro de un circuito integrado de aplicación específica (**Application Specific Integrated Circuit**, ASIC) y eficiencia en la fabricación, permiten a los vendedores de **switches** para la LAN ofrecer continuamente productos más rápidos a precios comparables a los existentes. Así que no es muy posible que la **overengineering** sea remplazada por otras alternativas de QoS muy pronto.

Pero si las características de QoS en desarrollo para los **switches** LAN pueden ser liberadas sin actualizaciones costosas de **hardware** o complejos cambios a la administración de la red, los administradores de red pueden estar más inclinados a considerar implementar sistemas de QoS en vez de depender de la **overengineering**.

Probablemente una combinación de **overengineering** y características de QoS emergerán como la solución a escoger. Varios fabricantes están a favor de esta estrategia, diciendo que es mejor realizarle una **overengineering** a los problemas de la red con ancho de banda "inteligente", en vez de uno "crudo".

En la WAN el **overengineering** es menos practica. El descenso en los

costos del ancho de banda en la WAN hará que las altas velocidades sean más costeables, algo que mitiga la necesidad de QoS en la WAN. Sin embargo, los costos del ancho de banda seguirán siendo un gasto significativo para la mayoría de las compañías, así que el **overengineering** en la WAN nunca tendrá la importancia que en la LAN.

En lugar de la **overengineering**, los sistemas de priorización de datos y las colas proveen la mayoría de las herramientas de QoS disponibles hoy día. Los **routers** han soportado la priorización de datos y las colas por muchos años. Algunos **switches** Gigabit Ethernet son diseñados para soportarla, pero el software de gestión basado en políticas para controlar la tecnología no está disponible.

Los sistemas de priorización de datos pueden ser caracterizados como implícitos o explícitos. Con QoS implícita, un **router** o un **switch** automáticamente reserva los niveles de servicio basados en el criterio especificado por el administrador, como son el tipo de aplicación, protocolo o dirección de origen. Cada paquete entrante es examinado o filtrado para verificar que cumpla con el criterio especificado.

Casi todos los **routers** soportan QoS implícita. Muchos **switches** se

están diseñando para que provean QoS implícita, pero solo ofrecen capacidades limitadas de priorización. Por ejemplo los **switches** pueden priorizar basados en el tipo de VLAN y la dirección de destino u origen en vez de información de alto nivel como el tipo de aplicación o protocolo. Los sistemas de redes basados en políticas (**policy-based network**) brindarán capacidades de priorización más robustas a estos **switches**.

La QoS explícita, por el contrario, le permite al usuario o a la aplicación solicitar un nivel de servicio en particular y los **switches** y **routers** intentan cumplir con la solicitud. La **IP Precedence**, también llamada **IP Type Of Service** (ToS), puede convertirse en la técnica de QoS explicita más usada.

Como parte del protocolo IP v4, IP ToS reserva un campo en el paquete IP donde los atributos de retraso, rendimiento y confiabilidad del servicio pueden ser especificados. Las versiones de Winsock en MS Windows 98 y NT le permiten al administrador usar aplicaciones para configurar este campo. Con la excepción de aplicaciones para multimedia, pocas aplicaciones populares soportan IP ToS.

El **Resource Reservation Protocol** (RSVP) es más sofisticado que IP

ToS. RSVP especifica su propio mecanismo de señalización para comunicar los requerimientos de QoS de una aplicación a un **router**. Al igual que IP ToS no está ampliamente implementado por los fabricantes. Aunque algunos **routers** soportan RSVP, el protocolo no está considerado maduro para su amplia instalación debido a problemas de escalabilidad. RSVP imparte una carga significativa en los **routers** lo que puede degradar el desempeño.

La QoS implícita es probable que continúe siendo más popular que la QoS explícita para el futuro previsible. La QoS implícita no requiere mucho procesamiento del **router**. Más importante, cualquier técnica de QoS explícita es una potencial pesadilla de administración. Dado el caso, probablemente los usuarios finales quieran configurar sus aplicaciones para que soliciten el mejor nivel posible de servicio. Los administradores probablemente necesitarán establecer reglas para los usuarios y posiblemente hasta configurar una QoS por cada usuario.

Una vez que los datos son priorizados usando técnicas implícitas o explícitas, las colas y los algoritmos de colas son usados para proveer el apropiado o deseado QoS.

Las colas, que son simples áreas dentro de la memoria de un **router** o

switch, son configuradas para que contengan paquetes con diferentes prioridades. Un algoritmo de cola determina el orden en el cual paquetes almacenados en las colas son transmitidos. La idea es darle el mejor servicio al tráfico de alta prioridad mientras se asegura, en varios grados, que los paquetes de baja prioridad obtengan algo del servicio.

Si ocurre congestión, el sistema de colas no garantiza que los datos cruciales alcanzarán su destino a tiempo; éste solo se asegura que los paquetes de alta prioridad llegarán antes que los de baja prioridad.

Sistemas de QoS más sofisticados resuelven este problema con sistemas de reserva de ancho de banda, los cuales asignan cantidades predeterminadas de ancho de banda a colas individuales o grupos de colas. Esto asegura que el ancho de banda siempre estará disponible para las colas de alta prioridad. La QoS se garantiza a menos que los datos en una cola sobrepasen la cantidad de ancho de banda reservado. Si esto ocurre, el algoritmo usualmente permite que el ancho de banda de las colas de baja prioridad sea usado para las de alta prioridad y viceversa.

Los algoritmos básicos de colas transmiten paquetes desde una misma

cola en el orden PEPS (primero que entra, primero que sale). Las tramas grandes asociadas con una transferencia de archivos de alta prioridad pueden demorar a una aplicación de proceso de transacciones que procesa pequeñas cantidades de datos, aunque los paquetes de ambas aplicaciones estén clasificados como alta prioridad.

Algoritmos de colas más sofisticados intentan ser equitativos (**fair**). Por ejemplo el algoritmo **weighted fair queuing** (WFQ) de Cisco, diferencia entre aplicaciones que necesitan mucho y poco ancho de banda y distribuye este a todas las aplicaciones en igual cantidad. La mayoría de los fabricantes de **routers** han desarrollado algoritmos de colas únicos y usan sus propios términos para describirlos.

Una limitación fundamental de los **routers** y **switches** de hoy (1998) es el número pequeño de colas que los dispositivos tienen para la QoS. Mientras que cuatro colas son comunes, otras adicionales facilitarían una priorización más granular y mayor equidad. Por ejemplo, los administradores podrían establecer una cola para dar preferencia a los paquetes de alta prioridad que necesiten viajar hasta un destino lejano.

Per-flow queuing establece colas en base a cada flujo, lo cual significa que cada sesión de usuario obtiene su propia cola. Esta arquitectura se

ha implementado en algunos **switches;** pero tiene el inconveniente asociado al incrementar el número de colas, de incrementar la complejidad del **switch**, lo que lleva a un aumento de costos y complicación en la configuración y administración.

Los mecanismos de controlar y evitar la congestión (**congestion control and avoidance mechanisms**) son otros aspectos importantes de la QoS.

El control de la congestión permite a las estaciones finales el regular su tasa de transmisión y reducir el tráfico si la red rechaza paquetes. Los protocolos TCP/IP y SNA soportan el control de la congestión desde hace muchos años. Por sí solo, el control de la congestión hace muy poco para asegurar la QoS.

Sin embargo el control de la congestión se hace más poderoso cuando se junta con el de evitar la congestión. El evitar la congestión es relativamente nuevo en el mundo TCP/IP, pero se está convirtiendo rápidamente en una característica estándar para los **routers** del tipo **Internet Service Provider** (ISP) y **carriers**.

Random early detection (RED) ha emergido como un método

estándar para evitar la congestión. En su forma básica, el RED aleatoriamente rechaza paquetes cuando las colas se llenan, lo que causa que las estaciones finales decrementen su tasa de transmisión para que las colas no se desborden. El **Weighted RED** (WRED) mejora al RED porque rechaza los paquetes basados en el IP ToS.

El modelado de paquetes (**traffic shaping**) se refiere a una variedad de técnicas para la modificación y manipulación de datos que ayuden a asegurar la QoS, como la segmentación de paquetes. Una de las razones por la que las redes ATM proporcionan una alta QoS es debido al uso de paquetes pequeños, o celdas. La cantidad máxima de tiempo que cualquier celda es retrasada es el tiempo que se tarda en transmitir una celda.

Tomado como préstamo de ATM, los fabricantes de **routers** y **switches** están adicionando capacidades de segmentación a sus productos. Por ejemplo Cisco en sus **routers** serie 12000 internamente segmenta los paquetes que atraviesan su **backplane** en paquetes de 64 **bytes**, lo cual ayuda a asegurar una QoS consistente dentro del **router**. Varios fabricantes de equipos Frame Relay segmentan los paquetes para su transmisión sobre enlaces WAN como una medida que asegura un envío predecible y un retraso mínimo.

La medición del tráfico (**traffic metering**) es otra forma de **traffic shaping**. Varios protocolos, como AppleTalk, tienen una tendencia a transmitir paquetes de forma desigual, lo que se conoce como la creación de “trenes” de paquetes (**trains of packets**). La técnica del **traffic metering** les da espacio a los “trenes” antes de la transmisión, por el almacenamiento temporal en un **buffer** de los paquetes, para asegurarse que la red no será sobrecargada. Esta técnica puede ser utilizada en los bordes de una red para mitigar los efectos de las ráfagas (**burst**).

No importa cuales capacidades de QoS un **router** o **switch** implementen, los dispositivos trabajan por sí solos para llevar los datos hasta su destino. Por ejemplo, un paquete puede pasar por los primeros dispositivos y enlaces sin problemas, y luego encontrar un enlace que impide que una adecuada QoS sea provista. Debido a que los dispositivos que el paquete ya ha atravesado funcionan independientemente, ellos pueden tomar los pasos para evitar el enlace defectuoso.

Pero los próximos sistemas de administración basados en políticas (**policy-based management**) son los que en definitiva unirán todas las

capacidades de QoS descritas anteriormente en un sistema consistente que asegure la QoS de extremo a extremo.

Los servidores de políticas (**policy servers**) en conjunto con las aplicaciones existentes para el monitoreo y administración de la red vigilarán la red para determinar las configuraciones óptimas de QoS y así configurar dinámicamente a los **routers** y **switches**.

Los servidores de políticas también consultarán los directorios de red, como el **Novell Directory Services**, para determinar los niveles de servicios apropiados que determinados usuarios y aplicaciones requieran. Estos servidores y los directorios típicamente usarán el **Lightweight Directory Access Protocol** (LDAP) para comunicarse.

Un apropiado diseño de la red es crucial para tener éxito con una implementación. La QoS es muy costosa y compleja para implementarla en todas partes, y aun las capacidades más robustas de la QoS no pueden vencer a un diseño de red deficiente. En las redes de campus, tiene más sentido implementar la QoS en el **backbone**. En las WAN, la QoS es más conveniente para los extremos de la red.

2.2 SOLUCIONES DEL IETF[2]

El **Internet Engineering Task Force** (IETF) ha venido trabajando en la definición de modelos de QoS para Internet por muchos años. La tarea no ha sido fácil, ya que los paquetes deben atravesar muchas redes y los proveedores deben estar de acuerdo no solo en cómo se gestiona la QoS, sino además en cómo se paga. Las principales técnicas desarrolladas por el IETF son las siguientes.

Integrated Services (Int-Serv)

Éste es un modelo para proveer QoS en Internet e intranets. La intensión de los diseñadores fue reservar alguna porción del ancho de banda de la red para tráfico como la voz y vídeo en tiempo real que requieren bajo retardo y ancho de banda garantizado. El grupo **Int-Serv Working Group** desarrolló el protocolo **Resource Reservation Protocol** (RSVP), que es un mecanismo para especificar requerimientos de QoS a lo largo de una red. Int-Serv tiene problemas de escalabilidad y fue muy difícil de implementar en la Internet. Sin embargo RSVP es usado en las redes empresariales y su mecanismo para configurar el ancho de banda a lo largo de la red está siendo usado en nuevas formas con MPLS.

2 SHELDON, Tom. Encyclopedia of Networking and Telecommunications. Estados Unidos : McGraw-Hill, 2001.

Differentiated Services (Diff-Serv)

Clasifica y marca paquetes de manera que reciban un siguiente salto específico en cada dispositivo de la red a lo largo de la ruta. Lo importante es que Diff-Serv realiza el trabajo en los extremos de forma que los dispositivos de red solo necesitan involucrarse en la formación de colas y reenvío de los paquetes. Diff-Serv trabaja al nivel IP para proveer QoS basado en las configuraciones del **Type of Service** (ToS).

Multiprotocol Label Switching (MPLS)

Es un protocolo, diseñado principalmente para redes del núcleo de Internet, que está pensado para proveer administración de ancho de banda y QoS para IP y otros protocolos. El control del núcleo de las redes es realizado por la construcción de **label switched path** (LSP) a lo largo de la red y el rápido reenvío de paquetes IP a lo largo de la red a través de los LSP. Por el etiquetado de paquetes (**labeling**) con un indicador del LSP que estos tienen que atravesar, es posible eliminar la sobrecarga de inspeccionar paquetes en cada dispositivo de la red a lo largo de la ruta. Los LSP son similares a los circuitos virtuales en redes ATM y Frame Relay. Se pueden utilizar aproximaciones a la ingeniería de tráfico (**traffic engineering**) para crear LSP que entreguen un determinado nivel de servicio.

2.3 CLASE DE SERVICIO (COS)

La Clase de Servicio (**Class of Service**, CoS) es una forma de proporcionar tratamiento preferencial a algunos tipos de tráfico bajo condiciones de congestión temporal en los enlaces de salida.

2.4 BALANCEO DE CARGAS

Con el balanceo de cargas (**load balancing**) los enlaces y/o servicios de la red son previstos para esparcir la carga a través de enlaces o sistemas redundantes. En un sitio **web**, el tráfico puede llegar sobre múltiples enlaces agregados (**multiple aggregate links**) a un sistema de balanceo de carga que entregará los paquetes al servidor menos ocupado o al más apropiado para procesar el paquete.

2.5 REDES PRIVADAS VIRTUALES

Las redes privadas virtuales (**Virtual Private Network**, VPN) es una técnica de **tunneling** que puede proveer QoS en algunos ambientes de redes. Protocolos como MPLS pueden proveerla sobre Internet.

3 SOPORTE WAN EN CISCO

3.1 ROUTERS SERIE 2600

La serie Cisco 2600 es una familia de **routers** de acceso multiservicio modular, provee configuraciones LAN y WAN flexibles, múltiples opciones de seguridad y un rango de procesadores de alto desempeño. Este rango de características hacen a la familia Cisco 2600 los **routers** ideales para sucursales de oficinas.

Las últimas adiciones a la familia Cisco 2600 de **routers** modulares incluyen a los modelos Cisco 2600 XM y el Cisco 2691. Estos modelos entregan un desempeño extendido, alta densidad, desempeño en la seguridad mejorado e incremento al soporte de aplicaciones concurrentes.

Los **routers** Cisco 2600 ofrecen versatilidad, integración y poder. Con mas de 70 módulos de red (**network modules**) e interfases, la arquitectura modular de la serie 2600 permite fácilmente a las interfases el ser actualizadas para acomodar la expansión de la red.

La serie Cisco 2600 comparte interfases modulares con los **routers** Cisco serie 1600, 1700, 3600 y 3700, proporcionando a los administradores de red y proveedores de servicios una solución de costo efectiva para las necesidades de las sucursales de hoy. En la tabla 1 se pueden observar las características de los modelos que integran esta serie.

Tabla 1 : Modelos de la familia de routers Cisco 2600[3]

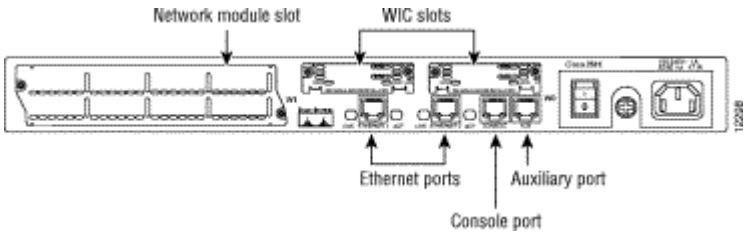
Plataforma	**NM**	**AIM**	**WIC**	**Interfases LAN** (FE=FastEthernet, TR= TokenRing)	**Desempeño** (Kpps)	**DRAM** (Default MB/Max MB)	**FLASH** (Default MB/Max MB)
CISCO2610/11	1	0	2	1 E/2 E	15	32/64	8/16
CISCO2620/21	1	0	2	1 FE/2 FE	25	32/64	8/32
CISCO2650/51	1	0	2	1 FE/2 FE	37	32/64	8/32
CISCO2610XM/11XM	1	1	2	1 FE/2 FE	20	96/128	32/48
CISCO2612	1	1	2	1TR/1 E	15	32/64	8/16
CISCO2620XM/21XM	1	1	2	1 FE/2 FE	30	96/128	32/48
CISCO2650XM/51XM	1	1	2	1 FE/2 FE	40	128/128	32/48
CISCO2691	1	2	3	2 FE	70	128/256	32/128

En los **routers** de la serie Cisco 2600 se puede elegir entre interfaces Ethernet, Token Ring y LAN Ethernet 10/100 con detección automática. Además, todos los modelos cuentan con dos ranuras para tarjetas de interfaz WAN (**WAN Interface Cards**, WIC), una ranura para módulos de red (**Network Module**, NM) y una ranura de módulo de integración avanzada (**Advanced Integration Module**, AIM), además de un puerto de consola de 115,2 Kbps y un puerto asíncrono auxiliar de

3 Cisco Systems. Cisco 2600 Series Multiservice Platforms. Estados Unidos : Cisco Systems, 2001. Disponible en: www.cisco.com/univercd/cc/td/doc/pcat/2600.htm

115,2 Kbps. En la figura 1 se puede ver un diagrama donde se indican sus localizaciones.

Figura 1 : Panel trasero en routers Cisco 2600



Módulos de red

Los módulos de red (**Network Module**) permiten personalizar los **routes** para que satisfagan las necesidades de casi cualquier sucursal. Estos módulos admiten una amplia gama de aplicaciones, entre las que se incluyen la integración multiservicio de voz y datos, acceso telefónico ISDN y análogo, acceso ATM, integración de conmutación de baja densidad, sistemas de detección de intrusos, etc.

Tarjetas de interfaz WAN

Las ranuras de las tarjetas de interfaz WAN (**WAN Interface Cards,** WIC) de la serie Cisco 2600 admiten 20 WIC, incluyendo las tarjetas de interfaz Voz/WAN Multiflex de uno o dos puertos y las tarjetas seriales de interfaz WAN de dos puertos para maximizar la densidad de interfaces y la eficacia de las ranuras.

Módulo de integración avanzada

El módulo de integración avanzada (**Advanced Integration Module,** AIM) es una ranura interna del **router** que utiliza **hardware** para funciones específicas de forma que libere de estas al procesador principal del **router**. El puerto AIM tiene acceso a casi todos los recursos del **router**, incluyendo al bus del sistema.

Ver el anexo D para conocer en detalle los WIC, NM y AIM que pueden instalarse en los router 2600.

Noticia importante. Los **routers** Cisco 2610, 2611, 2620, 2621, 2650 y 2651 han sido reemplazado por los **routers** Cisco 2600XM, los cuales fueron lanzados en mayo del 2002. Estos productos han alcanzado el estado de **end-of-sale** o **end-of-life**; no pueden hacerse pedidos y no serán soportados más. Para más información consultar el boletín del producto número 1958, disponible en: www.cisco.com/warp/public/cc/pd/rt/2600/1958_pp.htm.

Para más información de los **routers** Cisco serie 2600, incluyendo los modelos Cisco 2600XM, 2691 y los descontinuados, visitar los siguientes URL:

www.cisco.com/en/US/products/hw/routers/ps259/index.html

www.cisco.com/univercd/cc/td/doc/pcat/2600.htm

3.2 PROTOCOLOS WAN EN CISCO IOS

El software Cisco IOS Release 12.3 provee un rango de capacidades **Wide Area Network** (WAN) que se adecua a casi cualquier necesidad en una red. Cisco ofrece[4] **cell relay** mediante **Switched Multimegabit Data Service** (SMDS), conmutación de circuitos mediante RDSI/ ISDN, conmutación de paquetes mediante Frame Relay, y los beneficios de la conmutación de circuitos y paquetes con ATM. **LAN emulation** (LANE) provee conectividad entre ATM y otros tipos de LAN.

3.2.1 ATM

Es una tecnología de multiplexación y conmutación de celdas diseñada para combinar los beneficios de la conmutación de circuitos (retraso constante en la transmisión y capacidad garantizada) con aquellos de la conmutación de paquetes (flexibilidad y eficiencia para tráfico intermitente).

ATM es un ambiente orientado a la conexión. Todo el tráfico desde o hacia una red ATM está precedido por un **virtual path identifier** (VPI) y un **virtual channel identifier** (VCI). Un par VPI-VCI es considerado un **virtual circuit** (VC). Cada VC es una conexión privada hacia otro nodo en la red ATM. Cada VC es tratado como

4 Cisco Systems. Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2. Estados Unidos : Cisco Systems, 2001. Páginas WC-1 a WC-16.

un mecanismo punto a punto o punto a multipunto hacia otro **router** o **host** y es capaz de soportar tráfico bidireccional.

Cada nodo ATM tiene que establecer una conexión separada hacia cada nodo en la red ATM con el que necesita comunicarse. Todas estas conexiones son establecidas por medio de un **permanent virtual circuit** (PVC) o un **switched virtual circuit** (SVC) con un mecanismo de señalización ATM. Esta señalización está basada en la especificación **User-Network Interface** (UNI) del ATM Forum.

Cada VC se considera un enlace completo y separado hacia un nodo de destino. Los usuarios pueden encapsular los datos como los necesiten a través de la conexión. La red ATM presta poca atención al contenido de los datos. El único requerimiento es que los datos sean enviados a la tarjeta procesadora ATM del **router** en una manera que cumpla con el formato específico de la cada **ATM adaptation layer** (AAL).

Una AAL define la conversión de la información del usuario en celdas. Una AAL segmenta la información de las capas superiores dentro de celdas en el transmisor y reensambla las celdas en el receptor. AAL1 y AAL2 manejan el tráfico isócrono, como la voz y el vídeo, y solo son relevantes al **router** cuando está equipado ya sea con una tarjeta de interfaz ATM CES (**circuit emulation service**), o cuando tiene voz sobre las capacidades de AAL2. AAL3/4 soporta las

comunicaciones de datos, esto es, segmentar y reensamblar paquetes.

Una conexión ATM se usa simplemente para transferir flujos de **bits** de información hacia un **router** o **host** de destino. El **router** ATM toma la trama **common part convergence sublayer** (CPCS), la corta en celdas de 53 **bytes**, y las envía hacia el **router** o **host** de destino para reensamblar. En el formato AAL5, 48 bytes de cada celda son usados para los datos CPCS; los restantes 5 **bytes** son usados para el enrutamiento de la celda. El encabezado de la celda de 5 **bytes** contiene el par VPI-VCI de destino, el tipo de carga (**payload type**), **cell loss priority** (CLP) y el control de error del encabezado (**header error control**, HEC).

La red ATM es considerada una LAN con una disponibilidad alta de ancho de banda. Cada nodo final en una red ATM es un **host** en una subred específica. Todo nodo final que necesite comunicarse con otro debe estar en la misma subred dentro de la red.

De forma diferente a la LAN, la cual no es orientada a la conexión, ATM requiere de ciertas características para proveer un ambiente de LAN a los usuarios. Una de estas características es la capacidad de **broadcast**. Los protocolos que deseen difundir paquetes a todas las estaciones en una subred se les debe permitir hacerlo con una simple llamada a la capa 2. Para soportar el **broadcasting**, el

router debe permitir al usuario especificar un VC en particular como un VC de **broadcast**. Cuando el protocolo pase un paquete con una dirección de **broadcast** a los controladores, el paquete es duplicado y enviado a cada VC marcado como un VC de **broadcast**. Este mecanismo es conocido como **pseudobroadcasting**.

A partir del Cisco IOS Release 11.0, la señalización punto a multipunto permite que el **pseudobroadcasting** sea eliminado. En **routers** con señalización punto a multipunto, este puede configurar llamadas entre el mismo y múltiples destinos; los controladores no necesitan la duplicación de los paquetes de **broadcast**. Un solo paquete puede ser enviado al **switch** ATM, el cual lo replica hacia múltiples **hosts** ATM.

Medios de acceso

Cisco provee acceso ATM de las siguientes formas, dependiendo del **hardware** disponible en el **router:**

- ATM Inverse Processor

En los **routers** Cisco serie 7500, las interfases de red residen en procesadores de interfaz modular (**modular interface processors**), los cuales proveen una conexión directa entre el **Cisco Extended Bus** (CxBus) de alta velocidad y la red externa. Cada **ATM Inverse Processor** (AIP) provee una sola interfaz de red ATM; el máximo número de AIP que los **routers** Cisco 7500 soportan depende del ancho de banda configurado. El ancho de banda total a través de todos los AIP

del sistema debe estar limitado a 200 Mbps **full-duplex** (dos **Transparent Asynchronous Transmitter/ Receiver Interfaces** {TAXI}, o una SONET y un E3, o una SONET y una SONET usada poco, cinco E3, o cuatro T3).

- ATM Port Adapter, Enhanced Port Adapter, y ATM-CES Port Adapter

El **ATM port adapter** y el **ATM enhanced port adapter** están disponibles en los **routers** Cisco serie 7200 y en la segunda generación de los **Versatile Interface Processor** (VIP2) de los **routers** Cisco serie 7500. El **ATM-CES port adapter** solo esta disponible en los **routers** Cisco serie 7200.

- Network Processor Module

Los **routers** Cisco 4500 y 4700 soportan un OC-3c **network processor module** (NPM) o hasta dos E3/DS3 NPM. Los **physical layer interface modules** (PLIM) que soportan SONET/ **Synchronous Digital Hierarchy** (SDH/SONET) de 155 Mbps están disponibles para fibra monomodo y multimodo.

- 1-Port ATM-25 Network Module

Este modulo de red esta disponible en los **routers** Cisco serie 2600 y 3600.

- ATM OC-3 Network Modules

Este modulo de red esta disponible en los **routers** Cisco serie 3600.

- Multiport T1/E1 ATM Network Module con Inverse Multiplexing over ATM

Este modulo de red esta disponible en los **routers** Cisco serie 2600 y 3600.

- Multiport T1/E1 ATM Port Adapter con Inverse Multiplexing over ATM

Este modulo de red esta disponible en los **routers** Cisco serie 7100, 7200 y 7500.

- Acceso ATM sobre una interfase serial

En los **routers** que no soportan el **hardware** descrito anteriormente, una interfaz serial puede ser configurada para encapsulación multiprotocolo sobre la **ATM-Data Exchange Interface** (ATM-DXI), como está especificado por el RFC 1483. Este estándar describe dos métodos para transportar tráfico de redes interconectadas multiprotocolo no orientado a conexión sobre una red ATM. Un método permite la multiplexación de múltiples protocolos sobre un solo **permanent virtual circuit** (PVC). El otro utiliza diferentes **virtual circuits** (VC) para transportar diferentes protocolos. La implementación Cisco soporta el transporte de AppleTalk, Banyan VINES, IP y Novell Internetwork Packet Exchange (IPX).

Si se configura el acceso ATM sobre una interfaz serial, un **ATM data service unit** (ADSU) se requiere para hacer lo siguiente:

- Proveer la interfaz ATM hacia la red
- Calcular la **DXI Frame Address** (DFA) a partir de los valores VPI y

VCI definidos para el protocolo o protocolos transportados en el PVC.

- Convertir los paquetes salientes en celdas ATM
- Reensamblar las celdas entrantes en paquetes

Funcionalidades implementadas

Esta sección provee un vistazo general de las características ATM disponibles en los medios de acceso: AIP, ATM port adapter, Enhanced ATM port adapter, ATM-CES port adapter, NPM, 1-port ATM-25 network module, ATM OC-3 network modules, y multiport T1/E1 ATM network module. Las siguientes características están disponibles en todas las tarjetas de interfaz, a menos que se indique lo contrario.

La aplicación Cisco IOS para ATM soporta las siguientes características:

- Colas de tasa múltiple. (No disponible en ATM port adapter, ATM-CES port adapter, enhanced ATM port adapter, y 1-port ATM-25 network module).
- **Segmentation and reassembly** (SAR) de hasta 512 **buffers** para el AIP, **reassembly** de hasta 512 **buffers** para el NPM, SAR de hasta 200 **buffers** para el ATM port adapter, y SAR de hasta 400 **buffers** para el ATM-CES port adapter. Cada **buffers** representa un paquete.
- Contadores por cada circuito virtual (**Per-virtual-circuit counters**), lo cual mejora la exactitud de las estadísticas que se muestran en la salida de los

comandos **show**, por el aseguramiento que los paquetes autonómamente conmutados (**autonomously switched packets**) son contados, lo mismo que los paquetes conmutados rápidos y procesados.

- Soporte de hasta 2048 circuitos virtuales en el AIP y ATM port adapter.
- Soporte de hasta 2047 circuitos virtuales en el ATM-CES port adapter.
- Soporte de hasta 4096 circuitos virtuales en el enhanced ATM port adapter.
- Soporte de hasta 1023 circuitos virtuales en el NPM.
- Soporte de hasta 2048 circuitos virtuales en el 1-port ATM-25 network module.
- Soporte de hasta 1024 circuitos virtuales en el ATM OC-3 network modules.
- Soporte de hasta 256 circuitos virtuales en cada interfase del multiport T1/E1 ATM network modules con **inverse multiplexing over ATM** (IMA) en **routers** Cisco serie 2600 y 3600.
- Soporte de hasta 512 circuitos virtuales en cada **User-Network Interface** (UNI) y 512 circuitos virtuales por enlace en cada interfaz IMA de un multiport T1/E1 ATM port adapter con inverse multiplexing over ATM en **routers** Cisco serie 7100, 7200, y 7500.
- Soporte para **permanent virtual path connections** (PVP).
- Soporte para AAL3/4 y AAL5 (AAL3/4 esta soportada en **routers** Cisco serie 4500 y 4700, y en los 7000 en la AIP solamente).
- Soporte para **fast-switched transparent bridging over ATM**. Ésta solo soporta paquetes encapsulados con AAL5-**Subnetwork Access Protocol**

(SNAP).

- Colas de excepción (**exception queue**), las cuales son usadas para reporte de eventos, como errores de CRC. (Disponible solamente en el AIP).
- Soporte para **operation**, **administration**, y **maintenance** (OAM) en **loopback** punto a punto y por segmentos, **Alarm Indication Signal** (AIS), y **Remote Defect Indication** (RDI) F4 **and** F5 **cells**.
- Colas en bruto (**raw queue**), que son usadas por todo el tráfico sin procesar sobre una red ATM. El tráfico **raw** incluye a las celdas OAM y a las **Interim Local Management Interface** (ILMI). Las celdas de señalización ATM no son consideradas **raw**. (Disponible solo en el AIP).
- Hasta 256 **buffers** de transmisión para fragmentación simultanea en el ATM port adapter.
- **Fast switching** de IP e IPX.
- Cross-connect CES estructurado y no estructurado. (Disponible solo en el OC-3/STM-1 ATM Circuit Emulation Service network module y el ATM-CES port adapter).
- Priorización del transporte ATM, incluyendo las siguientes clases de tráfico:
    - Servicio orientado a la conexión **real-time** y **non-real-time variable bit rate** (rt-VBR y nrt-VBR), adecuado para voz y vídeo.
    - Servicio orientado a la conexión **available bit rate** (ABR), para tráfico, como interconexión de LAN y conectividad TCP/IP que trabaja bien con retrasos variables.

- **Unspecifed bit rate** (UBR), como es reconocido por el ATM Forum, sin asignación de recursos o especificación de QoS.

- Soporte al protocolo ATM **Interim Local Management Interface** (ILMI) como lo específica el ATM Forum para incorporar capacidades de administración de red.
- **Cell-based inverse multiplexing** que permite a las celdas OAM proveer la administración y el monitoreo, el cual se realiza a través de enlaces **imuxed** (**inverse multiplexed**). De esta manera, un **router** Cisco con una funcionalidad ATM IMA puede intercambiar información de monitoreo, como la conectividad, **alarm indication signals** (AIS), y **loopback**.

3.2.2 Broadband Access: PPP y Routed Bridge Encapsulation

El software Cisco IOS soporta un amplio rango de características y aplicaciones que permiten a un agregador de banda ancha en la oficina central (**central office broadband aggregator**) proveer las capacidades de selección de servicio y red requerida para la entrega de servicios de banda ancha avanzados.

Las siguientes funciones y aplicaciones son soportadas:

- PPP over ATM. Habilita un **router** de sitio central de alta capacidad con una interfaz ATM el terminar múltiples conexiones PPP remotas. Los beneficios de esta incluyen la validación de seguridad por usuario, **IP address pooling**, y capacidad de selección del servicio.

- PPP over Ethernet (PPPoE) over ATM. Provee la habilidad de conectar una red de **hosts** sobre un simple dispositivo de acceso puente (**bridging-access**) a un concentrador de acceso remoto. Con este modelo, cada **host** utiliza su propia pila PPPoE, y al usuario se le presenta una interfaz de usuario familiar. El control de acceso, la facturación y la selección del servicio pueden ser configurados por cada usuario, en vez de cada sitio.
- PPPoE over Ethernet. Provee conexión directa a interfaces Ethernet. Esta especificación Ethernet puede ser usada por múltiples **hosts** en una interfase Ethernet compartida para abrir sesiones PPP hacia múltiples destinos con uno o más **modems** de puente.
- PPPoE over IEEE 802.1Q VLAN. Permite la conexión de un **router** con capacidad para VLAN con otro dispositivo de red que soporte VLAN.
- ATM Routed Bridge Encapsulation. Enruta IP sobre tráfico Ethernet **bridged** RFC 1483 desde un **stub-bridge LAN**. Aquí se reduce el riesgo de seguridad asociado con el **bridging** normal por la reducción del tamaño de la red no segura.
- ATM PVC range y routed bridge encapsulation subinterface grouping. Permite la configuración de un número de PVC de una sola vez, ahorrando tiempo de configuración y NVRAM y acelerando el tiempo de arranque.
- PPPoE RADIUS port identification. Permite a un **L2TP access concentrator** (LAC) y un **LT2P network server** (LNS) identificar y reenviar valores de atributos NAS-Port y NAS-Port-Type para PPPoE over ATM y PPPoE over

IEEE 802.1Q VLAN.

3.2.3 Frame Relay

La implementación Frame Relay de Cisco actualmente soporta el enrutamiento sobre IP, DECnet, AppleTalk, XNS, Novell IPX, CLNS, Banyan VINES y transparent bridging. Aunque el acceso Frame Relay fue inicialmente restringido a línea dedicadas, el acceso por marcación (**dialup**) ahora esta soportado.

El software Frame Relay soporta las siguientes capacidades:

- Soporte para las tres especificaciones implementadas generalmente de la **Local Management Interfaces** (LMI) de Frame Relay:
    - La especificación desarrollada conjuntamente por Northern Telecom, Digital Equipment Corporation, StrataCom y Cisco Systems
    - La especificación de señal Frame Relay adoptada por el ANSI en T1.617 anexo D.
    - La especificación de señal Frame Relay adoptada por el ITU-T en Q.933 anexo A.
- Conformidad con las recomendaciones del ITU-T serie I como la I.122, “Framework for Additional Packet Mode Bearer Services”.
    - La especificación de encapsulación Frame Relay adoptada por el ANSI, T1.618.
    - La especificación de encapsulación Frame Relay adoptada por el ITU-

T, Q.922 anexo A.

- Conformidad con la encapsulación del **Internet Engineering Task Force** (IETF) en concordancia con el RFC 2427, excepto el **bridging**.
- Soporte para el mecanismo de **keepalive**, grupo **multicast** y mensaje de estado, como sigue:
  - El mecanismo de **keepalive** provee un intercambio de información entre el servidor de red y el **switch** para verificar que los datos están fluyendo.
  - El mecanismo **multicast** provee al servidor de red con un **data-link connection identifier** (DLCI) local y uno **multicast**. Esta característica es específica de la implementación Cisco de la especificación conjunta de **Frame Relay**.
  - El mecanismo de estado provee un reporte de estado continuo en los DLCI conocidos por el **switch**.
- Soporte a PVC y SVC al mismo tiempo en los mismos **routers** o sitios.
- Soporte para **Frame Relay Traffic Shaping** en lo siguiente:
  - Imposición de tasa (**rate enforcement**) para circuitos individuales. La **peak rate** para el tráfico de salida puede ser ajustado al **committed information rate** (CIR) o cualquier otra tasa configurable por el usuario.
  - Contención de tráfico dinámica por cada circuito virtual. Cuando el paquete **backward explicit congestion notification** (BECN) indica una congestión en la red, la tasa de tráfico de salida es

automáticamente reducida; cuando la congestión se alivia, el tráfico de salida se aumenta de nuevo.

- Soporte avanzado de colas en cada circuito virtual. Colas configurables, colas de prioridad y colas con igual peso (**weighted fair**) pueden ser configuradas para cada circuito virtual.

- Transmisión de la información de congestión desde Frame Relay hacia DECnet Phase IV y CLNS. Este mecanismo avanza los **bits** de **forward explicit congestion notification** (FECN) desde la capa Frame Relay a los protocolos de capas superiores después de verificar el bit FECN en los DLCI entrantes. El avance del **bit** FECN esta habilitado por defecto en cualquier interfase que utilice la encapsulación Frame Relay. No se necesita ninguna configuración.
- Soporte para **Frame Relay Inverse ARP** como se describe en el RFC 1293 para los protocolos AppleTalk, Banyan VINES, DECnet, IP, and IPX, y para paquetes nativos **Hello** en DECnet, CLNP, y Banyan VINES. Esto permite a un **router** ejecutando Frame Relay descubrir la dirección del protocolo de un dispositivo asociado con un circuito virtual.
- Soporte para la conmutación Frame Relay, por lo cual los paquetes son conmutados basados en el DLCI (el equivalente Frame Relay de la dirección **Media Access Control**, MAC). Los **routers** son configurados como un **switch** DTE Frame Relay híbrido o un nodo de acceso Frame Relay DCE puro dentro de la red Frame Relay.

La conmutación Frame Relay es usada cuando todo el tráfico que llega sobre un DLCI puede ser enviado hacia afuera sobre otro DLCI a la misma dirección de siguiente salto. En estos casos, el Cisco IOS no examina las tramas individualmente para descubrir la dirección de destino, y como resultado la carga de procesamiento en el **router** decrece.

La implementación de la conmutación Frame Relay de Cisco provee las siguientes funcionalidades:

- Conmutación sobre un túnel IP.
- Conmutación sobre **Network-to-Network Interfaces** (NNI) hacia otros **switches** Frame Relay.
- Conmutación **Local serial-to-serial**.
- Conmutación sobre los canales B de RDSI/ISDN.
- **Traffic shaping** en **switched** PVC.
- Manejo de la congestión en **switched** PVC.
- **Traffic policing** en **User-Network Interface** (UNI) DCE.
- Fragmentación FRF.12 en **switched** PVC.

- Soporte para subinterfases asociadas con una interfaz física. El software agrupa uno o más PVC bajo subinterfases separadas, las cuales a su vez están localizadas bajo una sola interfaz física.
- Soporte para **fast-path transparent bridging**, como se describe en el RFC

1490, para **Frame Relay encapsulated serial** y **High-Speed Serial Interfaces** (HSSI) en todas las plataformas.

- Soporte al **Frame Relay DTE MIB** especificado en RFC 1315. Sin embargo, la tabla de error no está implementada.
- Soporte para la fragmentación Frame Relay. Cisco ha desarrollado los tres tipos siguientes:
    - End-to-End FRF.12. Está definida por el FRF.12 Implementation Agreement. Este estándar fue desarrollado para permitir a las trama de datos grandes ser fragmentadas en piezas pequeñas y ser intercaladas con tramas de tiempo real. Ésta fragmentación es recomendada para usar con PVC que comparten enlaces con otros PVC que transportan voz y voz sobre IP (VoIP).
    - FRF.11 Anexo C. Cuando **Voice over Frame Relay,** VoFR (FRF.11) y la fragmentación están ambas configuradas sobre un PVC, los fragmentos Frame Relay son enviados en el formato FRF.11 Anexo C.
    - Propietaria de Cisco. Es usada en los paquetes de datos sobre un PVC que también se usa para tráfico de voz.

3.2.4 Frame Relay - ATM Internetworking

Cisco IOS soporta el acuerdo de implementación del Frame Relay Forum para la interoperación de datos los protocolos ATM y Frame Relay. Hay dos tipos de interoperación Frame Relay – ATM:

- FRF.5 Frame Relay-ATM Network Interworking

  FRF.5 provee la funcionalidad de interoperación de red que permite a los usuarios finales Frame Relay comunicarse con una red ATM intermediaria que soporte FRF.5. La encapsulación multiprotocolo y otros procedimientos de capas superiores son transportados de manera transparente, igual que si estuvieran en líneas arrendadas. FRF.5 describe los requerimientos de interoperación de red entre **Frame Relay Bearer Services** y **Broadband ISDN** (BISDN) **permanent virtual circuit** (PVC) **services**.

- FRF.8 Frame Relay-ATM Service Interworking

  FRF.5 provee la funcionalidad de interoperación de servicio que permite a los usuarios finales Frame Relay comunicarse con un usuario final ATM. El tráfico es traducido por un convertidor de protocolo que provee comunicación entre equipos diferentes de Frame Relay y ATM. FRF.8 describe un mapeo de uno a uno entre un PVC de Frame Relay y un PVC de ATM.

3.2.5 SMDS

La implementación del Cisco del protocolo **Switched Multimegabit Data Service** (SMDS) está basada en la tecnología **cell relay** como se define el los avisos técnicos de Bellcore, los cuales están basados en el estándar IEEE 802.6. Se provee una interfaz hacia la red SMDS utilizando facilidades de transmisión de

alta velocidad DS1 o DS3. La conexión a la red es hecha mediante un dispositivo llamado SDSU (SMDS **digital service unit**). El SDSU se conecta a un **router** o un servidor de acceso a través de un puerto serial. Del otro lado el SDSU termina la línea.

La implementación de SMDS soporta los protocolos IP, DECnet, AppleTalk, XNS, Novell IPX, Banyan VINES, y OSI, y **transparent bridging**. También soporta la encapsulación SMDS sobre una interfaz ATM.

El enrutamiento de AppleTalk, DECnet, IP, IPX, e ISO CLNS es completamente dinámico; esto es que las tablas de enrutamiento son determinadas y actualizadas dinámicamente. El enrutamiento de los otros protocolos requiere que se establezca una tabla de rutas estáticas de vecinos SMDS en un grupo de usuario. Una vez que esta tabla este configurada, todos los **routers** y servidores de acceso interconectados proveen enrutamiento dinámico.

Se soportan múltiples subredes IP lógicas como se define en el RFC 1209. Éste RFC describe el enrutamiento IP sobre una nube SMDS en la cual cada conexión es considerada un **host** en una red privada específica, y apunta hacia casos donde el tráfico debe transitar desde una red a otra. También provee la **Data Exchange Interface** (DXI) con **heartbeat**. El mecanismo de **heartbeat** periódicamente genera una trama de encuesta **heartbeat**.

Cuando una dirección de **multicast** no está disponible a un destino, el **pseudobroadcasting** puede ser habilitado para emitir paquetes a esos destinos utilizando una dirección de **unicast**.

3.2.6 Link Access Procedure Balanced (LAPB) y X.25

X.25 es un grupo de especificaciones publicadas por el ITU-T. Estas especificaciones son estándares internacionales que son llamados formalmente recomendaciones. Las recomendaciones X.25 de la ITU-T definen cómo las conexiones entre el DTE y DCE son mantenidas para acceso a terminales remotas y comunicaciones de computadores. La especificación X.25 define protocolos para dos capas del modelo de referencia OSI. El protocolo definido para la capa de enlace de datos es el LAPB. La capa de red normalmente se le llama el **packet level protocol** (PLP), pero es comúnmente referido (aunque menos correcto) como el protocolo X.25.

El ITU-T actualiza sus recomendaciones periódicamente. Las especificaciones que datan de 1980 y 1984 son las versiones más comunes y actualmente en uso. Adicionalmente la ISO ha publicado el ISO 7776:1986 como un equivalente al estándar LAPB, y el ISO 8208:1989 como un equivalente a la recomendación ITU-T capa de paquete X.25 de 1984. El software Cisco X.25 sigue la recomendación ITU-T X.25 de 1984, a excepción del **Defense Data Network** (DDN) y **Blacker**

Front End (BFE) **operation**, que siguen la recomendación ITU-T X.25 de 1980.

En adición al proveer acceso de terminal remoto, el software Cisco X.25 provee transporte para protocolos de LAN (IP, DECnet, XNS, ISO CLNS, AppleTalk, Novell IPX, Banyan VINES, y Apollo Domain) y bridging.

El software Cisco X.25 provee las siguientes capacidades:

- Transporte de datagramas LAPB. LAPB es un protocolo que opera en la capa 2 (capa de enlace de datos) del modelo de referencia OSI. Ofrece un servicio de conexión confiable para el intercambio de datos (en unidades llamadas tramas) con cada **host**. La conexión LAPB es configurada para transportar un solo o múltiples protocolos. Los protocolos de datagramas (IP, DECnet, AppleTalk, y otros) son transportados sobre una conexión LAPB confiable, o varios datagramas de estos protocolos son encapsulados en un protocolo propietario y transportados sobre una conexión LAPB. Cisco también implementa el **transparent bridging** sobre la encapsulación multiprotocolo LAPB en interfases seriales.
- Transporte de datagramas X.25. X.25 puede establecer conexiones con múltiples **hosts**; estas conexiones son llamadas circuitos virtuales. Los protocolos de datagramas son encapsulados dentro de paquetes en un circuito virtual X.25. El mapeo entre las direcciones X.25 de un **host** y su dirección de protocolo de datagrama permite a estos datagramas ser

enrutados a través de una red X.25, permitiendo a una red X.25 transportar protocolos LAN.

- Conmutación X.25. Las llamadas X.25 pueden ser enrutadas basadas en sus direcciones X.25 ya sea entre interfases seriales en el mismo **router** (conmutación local) o a través de una red IP hacia otro **router**, usando X.25 sobre TCP (XOT). XOT encapsula los paquetes de nivel X.25 dentro de una conexión TCP, permitiendo al equipo X.25 estar conectado mediante una red basada en TCP/IP. Las características de conmutación X.25 proveen una forma conveniente para conectar equipos X.25, pero no provee las características y capacidades especializadas de una X.25 PDN.
- Canal ISDN D. El tráfico X.25 sobre el canal D, usando hasta 9.6 Kbps de ancho de banda, puede ser usado para soportar muchas aplicaciones. Por ejemplo, puede ser requerido como una interfase primaria donde tráfico interactivo esporádico de bajo volumen es el modo normal de operación.
- **Packet Assembler/Disassembler** (PAD). Las sesiones de usuario pueden ser transportadas a través de una red X.25 usando los protocolos PAD definidos por las recomendaciones X.3 y X.29 del ITU-T.
- **Qualified Logical Link Control** (QLLC). El software Cisco puede usar el protocolo QLLC para transportar tráfico SNA a través de una red X.25.
- **Connection-Mode Network Service** (CMNS). Es un mecanismo que usan las direcciones basadas en OSI **network service access point** (NSAP) para extender la conmutación local X.25 a medios no seriales (por ejemplo,

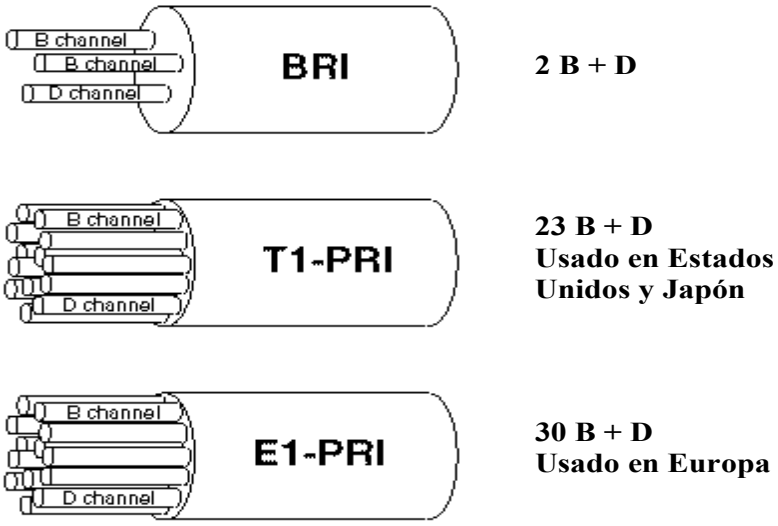
Ethernet, FDDI, y Token Ring). Esta implementación provee el X.25 PLP **over Logical Link Control type 2** (LLC2) para permitir conexiones sobre interfases no seriales. La implementación Cisco de CMNS soporta servicios definidos en el estándar ISO 8208 (**packet level**) y 8802-2 (**frame level**).

- DDN y BFE X.25. El DDN**-specified Standard Service** es soportado. Este servicio estándar es el protocolo requerido para usar con DDN **Packet-Switched Nodes** (PSN). La **Defense Communications Agency** (DCA) ha certificado a esta implementación del servicio para su anexo al DDN. La implementación DDN de Cisco también incluye la operación **Blacker Front End**.
- X.25 MIB. Subconjuntos de las especificaciones SNMP MIB Extension for X.25 LAPB (RFC 1381) y SNMP MIB Extension for the X.25 Packet Layer (RFC 1382) son soportadas. No están implementadas LAPB XID Table, X.25 **Cleared Circuit Table**, y X.25 **Call Parameter Table**. Todos los valores son de solo lectura.
- **Closed User Groups** (CUG). Un CUG es una colección de dispositivos DTE para los cuales la red controla el acceso entre dos miembros y entre un miembro y un no miembro. Una red X.25 puede soportar hasta 10.000 CUG. Los CUG permiten a varios suscriptores de red (dispositivos DTE) a ser segregados en subredes privadas que tienen accesos limitados de salidas y entradas.
- La implementación X.25 de Cisco no soporta el **fast switching**.

3.2.7 RDSI/ISDN

Los **routers** Cisco soportan[5] ISDN BRI e ISDN PRI. Ambos tipos de medios utilizan canales B y D. En la figura 2 se muestran cuantos canales B y D son asignados a cada tipo de medio.

Figura 2 : Relación entre los canales B y D de ISDN



ISDN BRI

Opera sobre la mayoría de los cables trenzados de cobre telefónicos. Provee un ancho de banda total de 144 Kbps mediante tres canales separados. Dos son los canales B que operan a 64 Kbps y son usados para transportar voz, vídeo, o tráfico de datos. El tercer canal, el canal D, es un canal de señalización de 16

5 Cisco Systems. Cisco IOS Dial Technologies Configuration Guide, Release 12.3. Estados Unidos : Cisco Systems, 2003.

Kbps usado para decirle a la **Public Switched Telephone Network** (PSTN) cómo manejar cada canal B. ISDN BRI es comúnmente conocida como “2 B + D”.

ISDN PRI

Esta diseñada para transportar grandes números de llamadas ISDN entrantes en **point of presences** (POP) y otros sitios centrales grandes. Toda la confiabilidad y rendimiento de ISDN BRI aplica a ISDN PRI, pero la ISDN PRI tiene 23 canales B de 64 Kbps cada uno y un canal D compartido de 64 Kbps que transporta tráfico de señalización. A ISDN PRI se le conoce comúnmente como “23 B + D” (en Norte América y Japón) o como “30 B + D” (en el resto del mundo).

El canal D notifica al **switch** de la oficina central a enviar las llamadas entrantes a **timeslots** particulares en el **router** o servidor de acceso Cisco. Cada uno de los canales B transporta datos o voz. El canal D transporta señalización para los canales B. El canal D identifica si la llamada es por un circuito conmutado digital o un **modem** análogo. Las llamadas de los **modems** análogos son decodificadas y luego enviadas a los **modems** de la tarjeta. Las llamadas por circuito conmutado digital son transmitidas directamente al procesador ISDN del **router**.

4 CONFIGURACIÓN DE ROUTERS CISCO 2600 PARA WAN

Entre los equipos de red con que cuenta la Universidad Tecnológica de Bolívar se cuentan **hubs**, **switches** y **routers**, los cuales se pueden utilizar en prácticas de laboratorio para configurar protocolos WAN. En la actualidad al contar con **routers** Cisco 2620 y 2621, se pueden realizar las prácticas con los protocolos Frame Relay y ATM utilizando las características de encapsulación de protocolos WAN en sus interfases seriales.

Acerca de las conexiones seriales

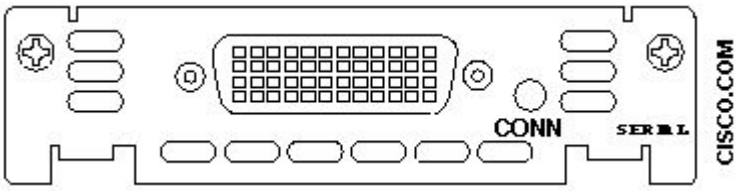
Las conexiones seriales pueden ser provistas por un módulo de red (**Network Module**, NM) o por tarjetas de interfaz WAN (**WAN Interface Card**, WIC), como se puede observar en el anexo D donde se detallan las tarjetas de expansión que pueden ser instaladas en la familia de **routers** Cisco 2600.

Los **routers** 2620 y 2621 con los que cuenta el laboratorio de redes de la UTB utilizan una tarjeta **1-Port Serial WAN Interface Card** (WIC-1T)[6] y cada **router**

6 Cisco Systems. Understanding the 1-Port Serial WAN Interface Card (WIC-1T). Estados Unidos: 2004. Disponible en: www.cisco.com/en/US/products/hw/modules/ps3129/products_tech_note09186a00800b0859.shtml

posee dos de estas tarjetas. Esta WIC provee conexiones seriales a sitios remotos o dispositivos seriales antiguos como sistemas de alarmas, concentradores **Synchronous Data Link Control** (SDLC) y dispositivos **packet over SONET** (POS). Solo provee un puerto serial. Utiliza el conector **Cisco 60-pin "5-in-1"**, este conector tiene una terminación DB-60 en un extremo y en el otro extremo puede ser: V.35, RS-232, RS-449, X.21 o EIE-530. En la figura 3 se observa un esquema de la WIC.

Figura 3 : Esquema de 1-Port Serial WAN Interface Card



Una opción para ampliar la capacidad de los **routers** para soportar más interfases (seriales o de otro tipo) es utilizar un módulo de red que tiene dos pequeños **slots** etiquetados como W0 y W1. Los **routers** 2600 pueden utilizar solamente el **2-WAN Interface Card Slot Network Module** (NM-2W), el cual es compatible con las siguientes WIC:

WIC-1T	WIC-1ADSL	VWIC-1MFT-G703
WIC-2T	WIC-1ADSL-I-DG	VWIC-2MFT-T1
WIC-1B-S/T	WIC-1SHDSL	VWIC-2MFT-T1-DI
WIC-1B-U	WIC-1AM	VWIC-2MFT-E1
WIC-1DSU-56K	WIC-2AM	VWIC-2MFT-E1-DI
WIC-1DSU-T1	WIC-1B-U-V2	
WIC-2A/S	VWIC-1MFT-T1	

Una de las partes más complicadas de configurar de un dispositivo de red (**router**, **switch**, **hub** o **access server**) es la selección de los cables seriales, para conectar éste dispositivo con los otros dispositivos seriales dentro de la red. Seleccionar el cable serial apropiado es fácil cuando se conocen las respuestas a estas tres preguntas:

¿El dispositivo de red se conectará a un dispositivo DTE o DCE?

¿Qué estándar de señalización requiere el dispositivo?

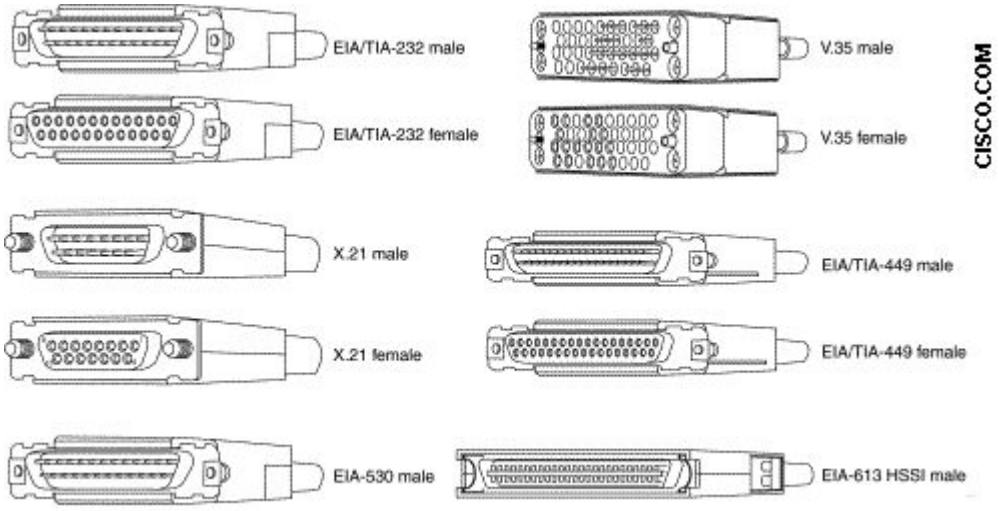
¿El tipo de conector que requiere el cable es macho o hembra?

Los dispositivos que se comunican sobre una interfaz serial están divididos en dos tipos: **data terminal equipment** (DTE) y **data communications equipment** (DCE). La diferencia más importante entre estos tipos de dispositivos es que los DCE suministran la señal del reloj (**clock signal**) que da el ritmo a las comunicaciones sobre el bus. La documentación que acompaña al dispositivo debe indicar si este es DTE o DCE (algunos dispositivos tienen un **jumper** o un comando por **software** para seleccionar el tipo). Si en la documentación no se indica, se puede tener una guía utilizando la siguiente tabla.

	DTE	**DCE**	**Seleccionable (DTE o DCE)**
Dispositivo	Terminales	Modems, CSU/DSU y Multiplexadores	Routers, Hubs, Switches y Access servers
Genero	Macho	Hembra	Cualquiera

Un número de diferentes estándares[7] definen la señalización sobre un cable serial, entre los cuales están EIA/TIA-232, X.21, V.35, EIA/TIA-449, EIA-530 y EIA-613 HSSI. Cada estándar define las señales sobre el cable y especifica el tipo de conector al final del cable. La documentación para el dispositivo a conectar debe indicar el estándar de señalización utilizado para el dispositivo. Pero si la documentación no lo informa, puede utilizar las ilustraciones que se muestran en la figura 4 para seleccionar el estándar de señalización requerido. Seleccione el conector que haga juego con el conector del dispositivo, no la ilustración que se parezca al conector del dispositivo.

Figura 4 : Conectores para cables seriales (macho/hembra)



Numeración de las interfases en routers 2600

Cada interfaz de red en un **router** Cisco 2600 está identificada por número de **slot**

7 Cisco Systems. Serial Cables. Estados Unidos : 2004. Disponible en: www.cisco.Com/ univercd/ cc/td/doc/pcat/se____c1.htm

y número de puerto.

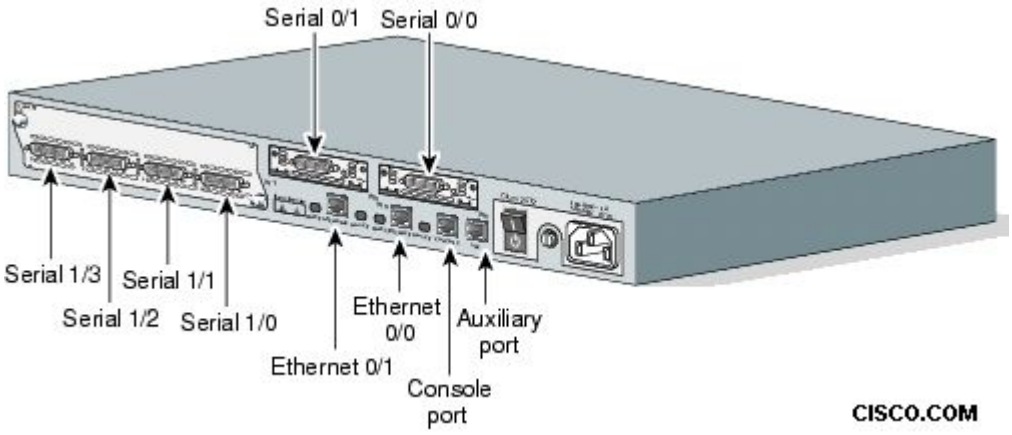
El chasis de los **routers** 2600 contiene un solo **slot** en el cual se puede instalar un módulo de red, este **slot** siempre es numerado como 1. Los dos **slots** para las WIC (W0 y W1) son siempre numerados como **slot** 0.

Los números de puerto[8] identifican a las interfases dentro de los módulos de red y WIC instalados en el **router**. Los números de puerto empiezan en 0 para cada **slot** y continúan de derecha a izquierda y si es necesario de abajo hacia arriba.

Los módulos de red y WIC son identificados inequívocamente por: tipo de interfase, número de **slot**, el símbolo "*/*" y el número de puerto. En la figura 5 se muestra un **router** de ejemplo donde se utiliza un módulo de red en el slot 1 con 4 interfases seriales.

8 Cisco Systems. Overview of Cisco Network Modules.Estados Unidos : Cisco Systems, 2004. Disponible en: www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/nm_inst/nm-doc/ovrnetm.htm

Figura 5 : Ejemplo de numeración de interfases en routers 2600



De la configuración anterior se obtiene la siguiente numeración de interfases:

Primera interfaz Ethernet	Ethernet 0/0
Segunda interfaz Ethernet	Ethernet 0/1
Slot W0: interfase serial 0	Serial 0/0
Slot W1: interfase serial 1	Serial 0/1
Slot 1: puerto serial asíncrono/síncrono 0	Serial 1/0
Slot 1: puerto serial asíncrono/síncrono 1	Serial 1/1
Slot 1: puerto serial asíncrono/síncrono 2	Serial 1/2
Slot 1: puerto serial asíncrono/síncrono 3	Serial 1/3

Luego de conocer las características principales de los recursos con los que se van a trabajar, se pasa a explicar la forma en que se realiza la configuración de los protocolos WAN escogidos (Frame Relay, ATM y RDSI) al utilizar la interfaz serial tipo WIC-1T de los **routers** 2620 y 2621.

4.1 PROTOCOLO FRAME RELAY

Frame Relay es un estándar[9] de la Unión Internacional de Telecomunicaciones (ITU) y del Instituto Nacional Americano de Normalización (ANSI) que define un proceso para el envío de datos a través de una red de datos públicos. Es una tecnología de datos eficiente, de elevado desempeño, utilizada en redes de todo el mundo. Frame Relay es una forma de enviar información a través de una WAN dividiendo los datos en paquetes. Cada paquete viaja a través de una serie de **switches** en una red Frame Relay para alcanzar su destino. Opera en las capas física y de enlace de datos del modelo de referencia OSI, pero depende de los protocolos de capa superior como TCP para la corrección de errores. Frame Relay se planteó originariamente como un protocolo destinado a utilizarse con las interfaces RDSI. Actualmente, Frame Relay es un protocolo de capa de enlace de datos conmutado de estándar industrial, que maneja múltiples circuitos virtuales mediante el encapsulamiento de control de enlace de datos de alto nivel (HDLC) entre dispositivos conectados. Frame Relay utiliza circuitos virtuales para realizar conexiones a través de un servicio orientado a conexión.

La red que proporciona la interfaz Frame Relay puede ser una red pública proporcionada por una portadora o una red de equipos privados, que sirven a una misma empresa. Una red Frame Relay puede componerse de computadores,

9 LAMMLE, Todd. CCNA: Cisco Certified Network Associate Study Guide 3 edition. Inglaterra : Sybex, 2002. 789 p. ISBN: 0-7821-4167-6.

servidores, etc., en el extremo del usuario y por dispositivos de red Frame Relay como **switches**, **routers**, **data service unit/channel service unit** (DSU/CSU) o multiplexores.

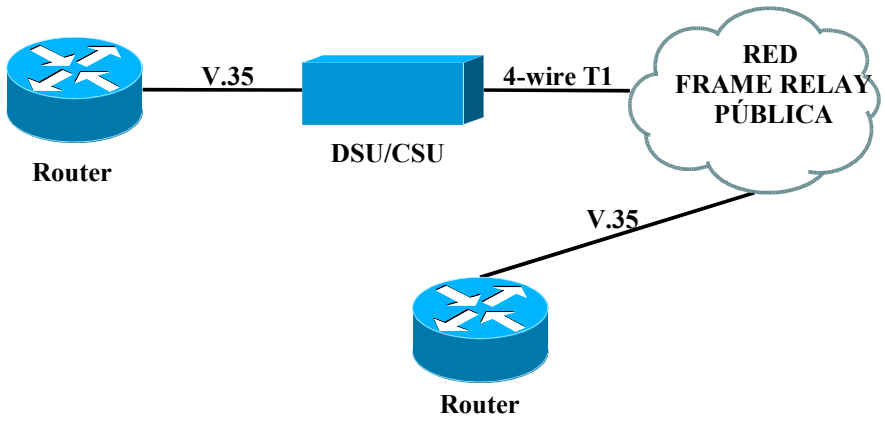
Configuración típica

Se pueden crear conexiones Frame Relay usando una de las configuraciones de **hardware** siguientes:

- **Routers** y servidores de acceso (**access servers**) conectados directamente al **switch** Frame Relay.
- **Routers** y servidores de acceso (**access servers**) conectados directamente a una DSU/CSU, la cual se conecta luego a un **switch** Frame Relay remoto.

La DSU/CSU convierte las señales V.35 o RS-449 a la señal de transmisión T1 codificada apropiadamente para que sea recibida a satisfacción por la red Frame Relay. La figura 6 ilustra las conexiones entre los componentes.

Figura 6 : Configuración Frame Relay típica



En las siguientes secciones se procede a explicar la forma en que se pueden configurar los **routers** para simular un red Frame Relay completa, es decir, donde se tengan **switches** que formen la "nube" del proveedor de servicios y **routers** que representen a los clientes que se conectan a ésta. Los **switches** se simulan al utilizar **Frame Relay Switching** empleando los mismos **routers** cómo se verá inmediatamente. Luego se procede a configurar **routers** de manera que se puedan conectar a la "nube de **switches**". En las partes finales de la configuración se presentan técnicas específicas del **software** Cisco IOS para la gestión del ancho de banda utilizando **Traffic Shaping**; para finalizar se ilustra como elaborar listas para marcar paquetes con el bit **Discard Eligibility** (DE) y el uso de la prioridad por DLCI. Luego de presentar todos los detalles acerca de configuraciones se procede a desarrollar varias prácticas de laboratorio para ilustrar los conceptos estudiados.

Procedamos a estudiar las configuraciones que ayudarán a la simulación de una red Frame Relay completa.

4.1.1 Configurar Frame Relay Switching[10]

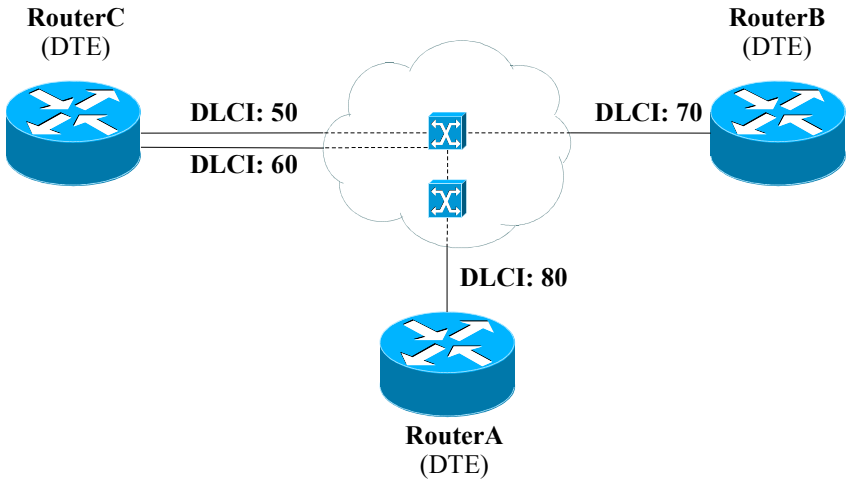
La conmutación Frame Relay (**Frame Relay Switching**) es una forma de conmutación de paquetes basada en el DLCI, el cual puede ser considerado el equivalente Frame Relay de las direcciones MAC. Se puede realizar el proceso de conmutación por la configuración de los **routers** o **access server** de Cisco dentro de una red Frame Relay. Dos partes constituyen una red de esta clase:

- Frame Relay DTE (el **router** o **access server**).
- Frame Relay DCE **switch**.

La figura 7 es una red Frame Relay conmutada. Los Routers A, B y C son Frame Relay DTE conectados entre sí mediante una red de **switches** Frame Relay.

10 Cisco Systems. Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2. Estados Unidos : Cisco Systems, 2001. Páginas WC-176 a WC-183.

Figura 7 : Red Frame Relay conmutada (Hub & Spoke)



El **Frame Relay Switching** es soportado por las interfases serial e ISDN, pero no por las subinterfases.

Lista de tareas

Para configurar **Frame Relay Switching** se deben realizar las siguientes tareas. Cada tarea es identificada como requerida u opcional.

- Habilitar **Frame Relay Switching** (Requerida).
- Configurar un dispositivo Frame Relay DTE, un **switch** DCE o soporte a NNI (Requerida).
- Crear los **switched** PVC (Requerida).
- Verificar **Frame Relay Switching** (Opcional).
- Localizar problemas (Opcional).

Habilitar Frame Relay Switching

Debe habilitar la conmutación de paquetes antes de poder realizar la configuración de un dispositivo Frame Relay DTE, DCE o con soporte para el protocolo **Network-to-Network Interface** (NNI). Para hacerlo debe usar el siguiente comando en modo de configuración global:

```
Router(config)# frame-relay switching
```

Configurar un dispositivo Frame Relay DTE, un switch DCE o soporte a NNI

Se puede configurar una interfase como un dispositivo DTE (opción por defecto) o como un **switch** DCE, o como un **switch** conectado a un **switch** para soportar conexiones NNI. Para hacerlo debe usar el siguiente comando en modo de configuración de interfase:

```
Router(config-if)# frame-relay intf-type [dce | dte | nni]
```

La opción NNI es la que normalmente se utiliza con menos frecuencia en la configuración de **routers**, en el caso de este documento se utiliza para simular las conexiones entre los **routers** que actúan o simulan ser **switches** Frame Relay dentro de la nube del proveedor de servicios Frame Relay.

Crear los switched PVC

Para crear los **switched** PVC con una ruta estática debe usar el siguiente comando en modo de configuración de interfase:

```
Router(config-if)# frame-relay route in-dlci interface out-
interface-type out-interface-number out-dlci
```

Descripción de los parámetros:

`in-dlci`. DLCI sobre el cual se recibe el paquete en esta interfaz.

`interface` `out-interface-type out-interface-number`. Interfase que se utilizará para transmitir el paquete.

`out-dlci`. DLCI que se utiliza para transmitir el paquete a través de la interfaz especificada.

Para crear un **switched** PVC en RDSI/ISDN se debe usar el siguiente comando en modo de configuración global:

```
Router(config)# connect connection-name interface dlci
{interface dlci | l2transport}
```

Descripción de los parámetros:

`connection-name`. Nombre para esta conexión.

`interface`. Interfase sobre la cual una conexión PVC será establecida.

`dlci`. Numero DLCI del PVC que será conectado.

`L2transport`. Especifica que el PVC no será un **switched** DLCI local, sino que será **tunneled** sobre el **backbone** de la red.

El siguiente ejemplo ilustra como habilitar **Frame Relay Switching** y definir una conexión llamada “conection_1” entre el DLCI 16 en la interfase serial 0/0 y el DLCI 100 en la interfase serial 0/1.

```
frame-relay switching
connect conection_1 serial 0/0 16 serial 0/1 100
```

Verificar Frame Relay Switching

Para verificar la correcta configuración se debe usar uno o más de los siguientes comandos:

- Mostrar estadísticas acerca de los PVC.

```
Router# show frame-relay pvc [interface interfaz] [dlci] [64-bit]
```

Descripción de los parámetros:

interface interfaz. Número de interfaz que contiene el DLCI para el cual se quiere mostrar la información de PVC.

dlci. Un DLCI específico usado en la interfaz. También muestra las estadísticas del PVC si se especifica solo.

64-bit. Muestra las estadísticas para los contadores de 64 **bits**.

Para obtener las estadísticas de los PVC en todas las interfases Frame Relay, utilice el comando sin parámetros.

Para obtener las estadísticas de los PVC que incluyan la configuración del **policy-map** o la prioridad configurada para un PVC, utilice este comando con el parámetro `dlci`. La tabla 2 provee un listado de todos los campos que se pueden desplegar al ejecutar este comando[11].

Tabla 2 : Campos de salida del comando show frame-relay pvc

Campo	Descripción
DLCI	One of the DLCI numbers for the PVC.
DLCI USAGE	Lists SWITCHED when the router or access server is used as a switch, or LOCAL when the router or access server is used as a DTE device.
PVC STATUS	Status of the PVC: ACTIVE, INACTIVE, or DELETED.
INTERFACE	Specific subinterface associated with this DLCI.
LOCAL PVC STATUS[1]	Status of PVC configured locally on the NNI interface.
NNI PVC STATUS[1]	Status of PVC learned over the NNI link.
input pkts	Number of packets received on this PVC.
output pkts	Number of packets sent on this PVC.
in bytes	Number of bytes received on this PVC.
out bytes	Number of bytes sent on this PVC.
dropped pkts	Number of incoming and outgoing packets dropped by the router at the Frame Relay level.
in FECN pkts	Number of packets received with the FECN bit set.
in BECN pkts	Number of packets received with the BECN bit set.
out FECN pkts	Number of packets sent with the FECN bit set.
out BECN pkts	Number of packets sent with the BECN bit set.
in DE pkts	Number of DE packets received.
out DE pkts	Number of DE packets sent.
out bcast pkts	Number of output broadcast packets.
out bcast bytes	Number of output broadcast bytes.
switched pkts	Number of switched packets.
no out intf[2]	Number of packets dropped because there is no output interface.
out intf down[2]	Number of packets dropped because the output interface is down.
no out PVC[2]	Number of packets dropped because the outgoing PVC is not configured.
in PVC down[2]	Number of packets dropped because the incoming PVC is inactive.
out PVC down[2]	Number of packets dropped because the outgoing PVC is inactive.
pkt too big[2]	Number of packets dropped because the packet size is greater than media MTU[3].
shaping Q full[2]	Number of packets dropped because the Frame Relay traffic-shaping queue is full.

11 Cisco Systems. Cisco IOS Wide-Area Networking Command Reference, Release 12.3. Estados Unidos : Cisco Systems, 2003. Página WR-568.

Campo	Descripción
pkt above DE[2]	Number of packets dropped because they are above the DE level when Frame Relay congestion management is enabled.
policing drop[2]	Number of packets dropped because of Frame Relay traffic policing.
pvc create time	Time at which the PVC was created.
last time pvc status changed	Time at which the PVC changed status.
VC-Bundle	PVC bundle of which the PVC is a member.
priority	Priority assigned to the PVC.
pkts marked DE	Number of packets marked DE because they exceeded the Bc.
policing Bc	Committed burst size.
policing Be	Excess burst size.
policing Tc	Measurement interval for counting Bc and Be.
in Bc pkts	Number of packets received within the committed burst.
in Be pkts	Number of packets received within the excess burst.
in xs pkts	Number of packets dropped because they exceeded the combined burst.
in Bc bytes	Number of bytes received within the committed burst.
in Be bytes	Number of bytes received within the excess burst.
in xs bytes	Number of bytes dropped because they exceeded the combined burst.
Congestion DE threshold	PVC queue percentage at which packets with the DE bit are dropped.
Congestion ECN threshold	PVC queue percentage at which packets are set with the BECN and FECN bits.
Service type	Type of service performed by this PVC. Can be VoFR or VoFR-cisco.
Post h/w compression queue	Number of packets in the post-hardware-compression queue when hardware compression and Frame Relay fragmentation are configured.
configured voice bandwidth	Amount of bandwidth in bits per second (bps) reserved for voice traffic on this PVC.
used voice bandwidth	Amount of bandwidth in bps currently being used for voice traffic.
service policy	Name of the output service policy applied to the VC.
Class	Class of traffic being displayed. Output is displayed for each configured class in the policy.
Output Queue	The WFQ[4] conversation to which this class of traffic is allocated.
Bandwidth	Bandwidth in kbps or percentage configured for this class.
Packets Matched	Number of packets that matched this class.
Max Threshold	Maximum queue size for this class when WRED is not used.
pkts discards	Number of packets discarded for this class.
bytes discards	Number of bytes discarded for this class.
tail drops	Number of packets discarded for this class because the queue was full.
mean queue depth	Average queue depth, based on the actual queue depth on the interface and the exponential weighting constant. It is a moving average. The minimum and maximum thresholds are compared against this value to determine drop decisions.
drops:	WRED parameters.
class	IP precedence value.
random	Number of packets randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence value.
tail	Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence value.
min-th	Minimum WRED threshold in number of packets.

Campo	Descripción
max-th	Maximum WRED threshold in number of packets.
mark-prob	Fraction of packets dropped when the average queue depth is at the maximum threshold.
Maximum Number of Hashed Queues	(Applies to class default only) Number of queues available for unclassified flows.
fragment type	Type of fragmentation configured for this PVC. Possible types are as follows: • end-to-end—Fragmented packets contain the standard FRF.12 header • VoFR—Fragmented packets contain the FRF.11 Annex C header • VoFR-cisco—Fragmented packets contain the Cisco proprietary header
fragment size	Size of the fragment payload in bytes.
adaptive active/inactive	Indicates whether Frame Relay voice-adaptive fragmentation is active or inactive.
time left	Number of seconds left on the Frame Relay voice-adaptive fragmentation deactivation timer. When this timer expires, Frame Relay fragmentation turns off.
cir	Current CIR in bps.
bc	Current committed burst (Bc) size, in bits.
be	Current excess burst (Be) size, in bits.
limit	Maximum number of bytes sent per internal interval (excess plus sustained).
interval	Interval being used internally (may be smaller than the interval derived from Bc/CIR; this happens when the router determines that traffic flow will be more stable with a smaller configured interval).
mincir	Minimum CIR for the PVC.
byte increment	Number of bytes that will be sustained per internal interval.
BECN response	Indication that Frame Relay has BECN adaptation configured.
pkts	Number of packets associated with this PVC that have gone through the traffic-shaping system.
frags	Total number of fragments shaped on this VC.
bytes	Number of bytes associated with this PVC that have gone through the traffic-shaping system.
pkts delayed	Number of packets associated with this PVC that have been delayed by the traffic-shaping system.
frags delayed	Number of fragments delayed in the shaping queue before being sent.
bytes delayed	Number of bytes associated with this PVC that have been delayed by the traffic-shaping system.
shaping	Indication that shaping will be active for all PVCs that are fragmenting data; otherwise, shaping will be active if the traffic being sent exceeds the CIR for this circuit.
shaping drops	Number of packets dropped by the traffic-shaping process.
Voice Queueing Stats	Statistics showing the size of packets, the maximum number of packets, and the number of packets dropped in the special voice queue created using the frame-relay voice bandwidth command queue keyword.
Discard threshold	Maximum number of packets that can be stored in each packet queue. Additional packets received after a queue is full will be discarded.
Dynamic queue count	Number of packet queues reserved for best-effort traffic.
Reserved queue count	Number of packet queues reserved for voice traffic.
Output queue size	Size in bytes of each output queue.
max total	Maximum number of packets of all types that can be queued in all queues.
Drops	Number of frames dropped by all output queues.

1. The LOCAL PVC STATUS and NNI PVC STATUS fields are displayed only for PVCs configured on Frame Relay NNI interface types. These fields are not displayed if the PVC is configured on DCE or DTE interface types.
2. The detailed packet drop fields are displayed for switched Frame Relay PVCs only. These fields are not displayed for terminated PVCs.
3. MTU = maximum transmission unit
4. WFQ = weighted fair queueing

- Mostrar todas las rutas Frame Relay configuradas con su estado actual.

```
Router# show frame-relay route
```

Este comando no posee parámetros. La siguiente tabla provee un listado de todos los campos que se pueden desplegar al ejecutar este comando.

Tabla 3 : Campos de salida del comando show frame-relay route

Campo	Descripción
Input Intf	Interfase de entrada.
Input Dlci	DLCI de entrada.
Output Intf	Interfase de salida.
Output Dlci	DLCI de salida.
Status	Estado de la conexión: active or inactive.

- Mostrar información acerca de la configuración en una interfaz.

```
Router# show interfaces [interfaz]
```

Localizar problemas

Para diagnosticar problemas con el **Frame Relay Switching,** se debe utilizar el siguiente comando en modo EXEC:

- Muestra mensajes **debug** para los **switched** PVC.

```
Router# debug frame-relay switching interface interfaz dlci
[interval segundos]
```

Descripción de los parámetros:

interface interfaz. Nombre de la interfaz Frame Relay

dlci. Número DLCI del **switched** PVC que será depurado.

interval segundos. Intervalo en segundos en el cual los mensajes de depuración serán actualizados.

Este comando solo puede ser usado con **switched** PVC. Las estadísticas de depuración son mostradas solo cuando hayan cambiado.

4.1.2 Configurar routers para Frame Relay

Una vez que se tenga una conexión confiable con el **switch** local Frame Relay en ambos extremos de un circuito virtual permanente (PVC), es tiempo de planear la configuración Frame Relay.

Lista de tareas

Para habilitar Frame Relay en una red se deben realizar las siguientes tareas básicas requeridas:

- Habilitar la encapsulación Frame Relay en una interfaz.
- Configurar el mapeo de direcciones dinámico o estático.

También se pueden realizar las siguientes tareas opcionales para adaptar Frame Relay a las necesidades particulares de una red:

- Configurar la LMI.

- Monitoreo y mantenimiento de las conexiones Frame Relay.

Habilitar la encapsulación Frame Relay en una interfaz

Para habilitar la encapsulación Frame Relay se debe usar el siguiente comando en modo de configuración de interfase:

```
Router(config-if)# encapsulation frame-relay [cisco |ietf]
```

Frame Relay soporta la encapsulación de todos los protocolos soportados de conformidad con el RFC 1490, lo que permite la interoperabilidad entre múltiples fabricantes. Se utiliza la forma de encapsulación Frame Relay del **Internet Engineering Task Force** (IETF) si el **router** o **access server** esta conectado a un equipo de otro fabricante a través de la red Frame Relay. La encapsulación IETF está soportada a nivel de interfase o por cada circuito virtual.

Configurar el mapeo de direcciones dinámico o estático

El mapeo de direcciones dinámicas utiliza Frame Relay **Inverse ARP** para solicitar la dirección de protocolo del siguiente salto (**next-hop protocol address**) para una conexión específica, dado un DLCI conocido. Las respuestas al **Inverse ARP** son registradas en una tabla de mapeo “direcciones a DLCI” en el **router** o **access server**; la tabla es usada luego para proporcionar la dirección de protocolo del siguiente salto o el DLCI para el tráfico saliente.

El **Inverse ARP** está habilitado por defecto para todos los protocolos que soporta, pero puede estar deshabilitado para pares protocolo/DLCI. Como resultado, se puede usar el mapeo dinámico para algunos protocolos y mapeos estáticos para otros protocolos en el mismo DLCI. Se puede deshabilitar explícitamente **Inverse ARP** para un par protocolo/DLCI si se conoce que el protocolo no está soportado en el otro extremo de la conexión.

- Configuración del mapeo de direcciones dinámico

  El **Inverse ARP** está habilitado por defecto para todos los protocolos habilitados en la interfaz física. No se envían paquetes para los cuales no hay protocolos habilitados en la interfaz. Debido a que el **Inverse ARP** está habilitado por defecto, no se necesita ningún comando adicional para configurar el mapeo dinámico en una interfaz.

- Configuración del mapeo de direcciones estático

  Un mapeo estático enlaza una dirección de protocolo de siguiente salto a un DLCI específico. Los mapeos estáticos eliminan la necesidad de las peticiones para **Inverse ARP**; cuando se provee un mapeo estático, el **Inverse ARP** se deshabilita automáticamente para el protocolo y DLCI especificado.

Se debe utilizar el mapeo estático si el **router** del otro extremo no soporta

Inverse ARP o no lo soporta únicamente para el protocolo que queremos usar sobre Frame Relay.

Para establecer un mapeo estático de acuerdo a las necesidades de la red, utilice el siguiente comando en el modo de configuración de interfaz:

```
Router(config-if)# frame-relay map protocol protocol-address
dlci [broadcast] [ietf] [cisco]
```

Descripción de los parámetros:

`protocol`. Uno cualquiera de los valores encerrados entre paréntesis: IP (**ip**), DECnet (**decnet**), AppleTalk (**appletalk**), XNS (**xns**), Novell IPX (**ipx**), VINES (**vines**), ISO CLNS (**clns**).

`protocol-address`. Dirección destino del protocolo.

`dlci`. Número DLCI usado para conectar a la dirección de protocolo especificada en la interfaz. Rango de números de 16 a 1007.

`broadcast`. Reenvía los **Broadcast** a esta dirección cuando los **Multicast** no están habilitados.

`ietf`. Utiliza la encapsulación Frame Relay del IETF.

`cisco`. Utiliza la encapsulación Frame Relay propietaria de Cisco.

Muchos DLCI pueden ser conocidos por un **router** y así pueden enviar datos a muchos lugares diferentes, pero estos son multiplexados sobre un enlace

físico. El mapeo de Frame Relay define una conexión lógica entre una pareja protocolo-dirección, y el DLCI correcto.

Los parámetros opcionales **ietf** y **cisco** permiten flexibilidad en la conexión. Si no se especifican, el mapeo hereda los atributos fijados con el comando **encapsulation frame-relay**. Se pueden usar las opciones de encapsulación para especificar, por ejemplo, que todas las interfases utilicen la encapsulación IETF excepto una, la cual necesita la encapsulación CISCO y que puede ser configurada utilizando la opción **cisco** del comando **frame-relay map**.

Configurar la LMI

Comenzando con la versión 11.2 de la aplicación Cisco IOS se soporta el **Local Management Interface** (LMI) **autosense**, el cual habilita a las interfases para determinar el tipo de LMI soportado por el **switch**. El soporte a LMI **autosense** significa que ya no es necesario configurar el LMI explícitamente.

Las siguientes secciones explican con mayor detalle la configuración del LMI.

- Activación del LMI **autosense**

El LMI **autosense** está activo en los siguientes casos:

Se enciende el **router** o el estado de la interfaz cambia a **up**.

El **line protocol** está **down**, pero **line** está **up**.

La interfaz es Frame Relay DTE.

El tipo de LMI no está configurado explícitamente.

La forma en que funciona la activación del LMI **autosense** es la siguiente:

Petición del estado: Cuando el LMI **autosense** está activo, envía una petición de estado completa, en los tres tipo de LMI, al **switch**. El orden es ANSI, ITU y CISCO, y es realizada de forma rápida. El **software** Cisco IOS provee la habilidad de escuchar simultáneamente en el DLCI 1023 (CISCO) y DLCI 0 (ANSI e ITU).

Mensajes de estado: Una o más de las peticiones de estado producirán una respuesta (mensaje de estado) por parte del **switch**. El **router** decodificará el formato de las respuestas y se configurará de forma automática. Si más de una respuesta es recibida, el **router** se configurará con el tipo de la última respuesta recibida. Esto es para acomodarse a los **switches** inteligentes que pueden manejar múltiples formatos simultáneamente.

LMI **autosense**: Si el LMI **autosense** no tiene éxito, un esquema inteligente de reintento está presente. Cada intervalo N391 (por defecto es 60 segundos, lo cual son 6 intentos de intercambios a 10 segundos cada uno), el LMI **autosense** intentará determinar el tipo de LMI.

La única indicación visible al usuario que el LMI **autosense** está ejecutándose es cuando se activa el **debug frame-relay lmi**. A cada intervalo N391, el usuario verá tres peticiones rápidas de estado saliendo de la interfaz serial: una ANSI, otra ITU y otra CISCO.

Opciones de configuración: No se ofrece ninguna opción; el LMI **autosense** es transparente al usuario. Se puede deshabilitar el LMI **autosense** por la configuración explícita del tipo LMI. El tipo de LMI debe escribirse al NVRAM de modo que la próxima vez que el **router** se encienda, el LMI **autosense** quede inactivo.

- Configuración explícita del LMI

EL **software** IOS para Frame Relay soporta los estándares aceptados de la industria para manejar el LMI, incluyendo la especificación de Cisco. Si desea configurar el LMI y por esto desactivar el LMI **autosense**, realice las siguientes tareas:

Fijar el tipo de LMI: Si el **router** o **access server** está conectado a una red pública de datos, el tipo de LMI debe concordar con el tipo usado por esta red. De otra forma, el tipo de LMI debe fijarse para satisfacer las necesidades de la red Frame Relay privada. Se puede fijar uno de los tres tipos de LMI en dispositivos Cisco: ANSI T1.617 Anexo D, CISCO e ITU-T Q.933 Anexo A. Para realizarlo utilice el siguiente comando en modo de

configuración de interfaz:

```
Router(config-if)# frame-relay lmi-type {ansi | cisco | q933a}
```

Fijar el intervalo de LMI **Keepalive**: Un intervalo de **Keepalive** debe ser fijado para configurar el LMI. Por defecto este intervalo es de 10 segundos y de acuerdo con el protocolo LMI debe ser menor que el correspondiente intervalo en el **switch**. Para fijar el intervalo de **Keepalive** utilice el siguiente comando en modo de configuración de interfaz:

```
Router(config-if)# keepalive segundos
```

Para deshabilitar los **Keepalive** en redes donde no se utiliza LMI, utilice el siguiente comando en modo de configuración de interfaz:

```
Router(config-if)# no keepalive
```

Monitoreo y mantenimiento de las conexiones Frame Relay

Para realizar el monitoreo de las conexiones Frame Relay, utilice cualquiera de los siguientes comando en el modo EXEC:

- Borrar el mapeo dinámico creado por el uso del **Inverse** ARP.

  ```
  Router# clear frame-relay-inarp
  ```

  Este comando no posee parámetros.

- Mostrar información de los DLCI y LMI en la interfase serial seleccionada.

  ```
  Router# show interfaces serial número
  ```

- Mostrar estadísticas del LMI.

```
Router# show frame-relay lmi [type number]
```

Descripción de los parámetros:

`type`. Tipo de interfaz, que debe ser **serial**.

`number`. Número de la interfaz.

Al introducir el comando sin parámetros se obtienen las estadísticas de todas las interfases Frame Relay. La siguiente tabla provee un listado de todos los campos que se pueden desplegar al ejecutar este comando.

Tabla 4 : Campos de salida del comando show frame-relay lmi

Campo	Descripción
LMI Statistics	Signalling or LMI specification: CISCO, ANSI, or ITU-T.
Invalid Unnumbered info	Number of received LMI messages with invalid unnumbered information field.
Invalid Prot Disc	Number of received LMI messages with invalid protocol discriminator.
Invalid dummy Call Ref	Number of received LMI messages with invalid dummy call references.
Invalid Msg Type	Number of received LMI messages with invalid message type.
Invalid Status Message	Number of received LMI messages with invalid status message.
Invalid Lock Shift	Number of received LMI messages with invalid lock shift type.
Invalid Information ID	Number of received LMI messages with invalid information identifier.
Invalid Report IE Len	Number of received LMI messages with invalid Report IE Length.
Invalid Report Request	Number of received LMI messages with invalid Report Request.
Invalid Keep IE Len	Number of received LMI messages with invalid Keep IE Length.
Num Status Enq. Sent	Number of LMI status inquiry messages sent.
Num Status Msgs Rcvd	Number of LMI status messages received.
Num Update Status Rcvd	Number of LMI asynchronous update status messages received.
Num Status Timeouts	Number of times the status message was not received within the keepalive time value.
Num Status Enq. Rcvd	Number of LMI status enquiry messages received.
Num Status Msgs Sent	Number of LMI status messages sent.
Num Status Enq. Timeouts	Number of times the status enquiry message was not received within the T392 DCE timer value.
Num Update Status Sent	Number of LMI asynchronous update status messages sent.

- Mostrar las entradas actuales para el mapeo Frame Relay e información de las conexiones.

```
Router# show frame-relay map
```

Este comando no utiliza parámetros. Utilice este comando para determinar si el **Inverse ARP** de Frame Relay resolvió una dirección remota a un DLCI local. Este comando no está habilitado para subinterfases punto a punto. Este es de utilidad para interfases y subinterfases multipunto.

Un ejemplo de la salida del comando es:

```
Router# show frame-relay map
Serial 1 (administratively down): ip 10.108.177.177 dlci 177
(0xB1,0x2C10), static, broadcast, CISCO, TCP/IP Header Compression
(inherited), passive (inherited)
```

Donde lo anterior significa:

Serial 1 (administratively down)	Identifica a una interfaz Frame Relay y su estado (**up** o **down**).
ip 10.108.177.177	Dirección IP de destino.
dlci 177 (0xB1,0x2C10)	DLCI que identifica la conexión lógica que se utiliza para acceder a está interfaz. Este valor es mostrado de tres formas: su valor decimal (177), hexadecimal (0xB1) y su valor como aparecería en el "cable" (0x2C10).
vc-bundle	PVC **bundle** que sirve como la conexión lógica que se usa para acceder a la interfase.
static/dynamic	Indica si la entrada es dinámica o estática.
Broadcast	Indica un seudo **broadcast**.
CISCO	Indica el tipo de encapsulación para este mapeo (**CISCO** o **IETF**).
TCP/IP Header Compression (inherited), passive (inherited)	Indica si las características de compresión del encabezado TCP/IP fueron heredadas desde la interfase o fueron configuradas explícitamente para el mapeo IP.
status defined, active	Indica que el mapeo entre la dirección de destino y el DLCI está activo.

- Mostrar estadísticas para los PVC.

```
Router# show frame-relay pvc
```

La explicación detallada de este comando se dio anteriormente.

- Mostrar las estadísticas del tráfico Frame Relay.

```
Router# show frame-relay traffic
```

Muestra estadísticas globales de Frame Relay desde la última vez que se reinició el **router**. No tiene parámetros.

- Mostrar mensajes **debug** para la LMI.

```
Router# debug frame-relay lmi
```

Este comando genera muy pocos mensajes y puede proveer respuestas a preguntas como:

¿Está el **router** comunicándose con el **switch** Frame Relay local?

¿Está el **router** obteniendo los mensajes de estado LMI completos para el PVC suscrito con el proveedor?

¿Son los DLCI correctos?

A continuación se presenta un ejemplo de la salida del comando para una conexión exitosa:

```
*Mar 1 01:17:58.763: Serial0(out): StEnq, myseq 92, yourseen 64, DTE up
*Mar 1 01:17:58.763: datagramstart = 0x20007C, datagramsize = 14
*Mar 1 01:17:58.763: FR encap = 0x0001030800 75 95 01 01 01 03 02 5C 40
```

```
*Mar 1 01:17:58.767:
*Mar 1 01:17:58.815: Serial0(in): Status, myseq 92
*Mar 1 01:17:58.815: RT IE 1, length 1, type 1
*Mar 1 01:17:58.815: KA IE 3, length 2, yourseq 65, myseq 92
*Mar 1 01:18:08.763: Serial0(out): StEnq, myseq 93, yourseen 65, DTE up
*Mar 1 01:18:08.763: datagramstart = 0x20007C, datagramsize = 14
*Mar 1 01:18:08.763: FR encap = 0x0001030800 75 95 01 01 01 03 02 5D 41
*Mar 1 01:18:08.767:
*Mar 1 01:18:08.815: Serial0(in): Status, myseq 93
*Mar 1 01:18:08.815: RT IE 1, length 1, type 1
*Mar 1 01:18:08.815: KA IE 3, length 2, yourseq 66, myseq 93
*Mar 1 01:18:18.763: Serial0(out): StEnq, myseq 94, yourseen 66, DTE up
*Mar 1 01:18:18.763: datagramstart = 0x20007C, datagramsize = 14
*Mar 1 01:18:18.763: FR encap = 0x0001030800 75 95 01 01 00 03 02 5E 42
*Mar 1 01:18:18.767:
*Mar 1 01:18:18.815: Serial0(in): Status, myseq 94
*Mar 1 01:18:18.815: RT IE 1, length 1, type 0
*Mar 1 01:18:18.819: KA IE 3, length 2, yourseq 67, myseq 94
*Mar 1 01:18:18.819: PVC IE 0x7 , length 0x3 , dlci 980, status 0x2
```

Note el estado del “DLCI 980” en la salida anterior. Los posibles valores para este campo de estado se explican a continuación[12].

0x0	Added/inactive means that the switch has this DLCI programmed but for some reason (such as the other end of this PVC is down), it is not usable.
0x2	Added/active means the Frame Relay switch has the DLCI and everything is operational. You can start sending it traffic with this DLCI in the header.
0x3	Is a combination of an active status (0x2) and the RNR (or r−bit) that is set (0x1). This means that the switch − or a particular queue on the switch − for this PVC is backed up, and you stop transmitting in case frames are spilled.
0x4	Deleted means that the Frame Relay switch doesn't have this DLCI programmed for the router. But it was programmed at some point in the past. This could also be caused by the DLCIs being reversed on the router, or by the PVC being deleted by the telco in the Frame Relay cloud. Configuring a DLCI (that the switch doesn't have) will show up as a 0x4.
0x8	New/inactive
0x0a	New/active

4.1.3 Configurar Frame Relay Traffic Shaping[13]

Al definir circuitos virtuales (VC) separados para diferentes tipos de tráfico y especificando colas y una tasa de tráfico de salida para cada VC, se puede proveer ancho de banda garantizado para cada tipo de tráfico. Al especificar tasas diferentes de tráfico para distintos VC sobre la misma línea, se puede realizar una multiplexación por división de tiempo (**time division multiplexing**, TDM) virtual. Al

12 Cisco Systems. Comprehensive Guide to Configuring and Troubleshooting Frame Relay. Estados Unidos, Cisco Systems, 2003.

13 Cisco Systems. Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2. Estados Unidos : Cisco Systems, 2001. Páginas WC-168 a WC-175.

contener el tráfico de salida desde las líneas de altas velocidades de las oficinas centrales a las líneas de bajas velocidades en las ubicaciones remotas, se puede aliviar la congestión y la perdida de datos en la red.

El modelado de tráfico (**Traffic Shaping**) aplica para los PVC y SVC. El **Traffic Shaping** no es efectivo para la conmutación de PVC de capa 2 (**Layer 2 PVC Switching)** cuando se usa el comando **frame-relay route**.

Para más información acerca de las capacidades de la implementación de **Frame Relay Traffic Shaping** por parte de Cisco y su lugar dentro de las técnicas de QoS de Cisco, leer el anexo B.

Lista de tareas

Para configurar **Frame Relay Traffic Shaping** realice las siguientes tareas:

- Habilitar la encapsulación Frame Relay en una interfaz (Requerida).
- Habilitar **Frame Relay Traffic Shaping** en una interfaz (Requerida).
- Configurar **Enhanced Local Management Interface**, ELMI (Opcional).
- Especificar un **Traffic-Shaping Map Class** para la interfaz (Opcional).
- Definir un Mapa de Clases (**Map Class**) con parámetros para colas y **Traffic Shaping** (Opcional).

Habilitar la encapsulación Frame Relay en una interfaz

Para habilitar la encapsulación Frame Relay debe usar el siguiente comando en modo de configuración de interfase:

```
Router(config-if)# encapsulation frame-relay [cisco |ietf]
```

Habilitar Frame Relay Traffic Shaping en una interfaz

Al realizar esta tarea, se habilitan de forma simultanea el **Traffic Shaping** y las colas por cada VC en todos los PVC y SVC de la interfaz. El **Traffic Shaping** permite al **router** controlar la tasa de salida del circuito y reaccionar a la información de notificación de congestión si se encuentra configurada. Para habilitar utilice el siguiente comando en modo de configuración de interfase:

```
Router(config-if)# frame-relay traffic-shaping
```

Para circuitos virtuales a los cuales no se les han especificado parámetros de colas o **Traffic Shaping**, un conjunto de valores por defecto son usados. La cola por defecto es FIFO.

Configurar ELMI

La **Enhanced Local Management Interface** (ELMI) permite al **router** aprender los parámetros de QoS y la información de conectividad desde un **switch** Cisco y utilizar esta información para la configuración y administración del **Traffic Shaping**, a esto se le llama **ELMI QoS autosense**. ELMI simplifica el proceso de

configurar **Traffic Shaping** en el **router** y reduce las posibilidades de especificar valores incorrectos o inconsistentes. ELMI funciona entre **routers** y **switches** Cisco (plataformas BPX e IGX).

Para habilitar ELMI utilice el siguiente comando en modo de configuración de interfase:

```
Router(config-if)# frame-relay QoS-autosense
```

Especificar un Traffic-Shaping Map Class para la interfaz

Al especificar una Frame Relay **map class** para una interfaz principal, todos los circuitos virtuales (VC) en sus subinterfases heredan los parámetros de **Traffic Shaping** definidos para la clase.

Para especificar un **map class** para la interfaz específica, utilice el siguiente comando en modo de configuración de interfaz:

```
Router(config-if)# frame-relay class name
```

Este comando se puede aplicar en interfases y subinterfases. Todos los parámetros relevantes definidos dentro del nombre (`name`) de este **map class** son heredados por cada circuito virtual creado en la interfaz o subinterfaz. Para cada circuito virtual, las reglas de precedencia son las siguientes:

1. Utilizar el **map class** asociado con el VC si existe.
2. Si no existe, utilizar el **map class** asociado con la subinterfase si el **map class** existe.
3. Si no, utilizar el **map class** asociado con la interfase si el **map class** existe.
4. Si no, utilizar los parámetros por defecto de la interfaz.

Se pueden sobrescribir los valores por defecto para un DLCI específico en una subinterfaz específica, al usar el comando de configuración de circuitos virtuales **frame-relay class** para asignar el DLCI explícitamente a una clase diferente.

Definir un Map Class y sus parámetros para colas y Traffic Shaping

Cuando se define un **map class** para Frame Relay, se pueden especificar las tasas promedio (**average**) y máxima (**peak**) en bits por segundo (bps) que se permiten en el VC asociado con la **map class**. También se puede especificar una **custom queue list** o un **priority queue group** para ser usado con el VC asociado con el **map class**. Para definir una **map class** utilice los siguientes comandos empezando en el modo de configuración global:

Definir una **map class**.

```
Router(config)# map-class frame-relay map-class-name
```

Después de especificar el nombre de la **map class**, se pueden especificar parámetros de QoS para la **map class** como por ejemplo: **committed information rate** (CIR) de entrada y salida, **committed burst rate** (Bc), **excess burst rate** (Be), e **idle timer**.

Para especificar una combinación protocolo y dirección a la cual se deben aplicar los parámetros de QoS, se debe asociar la **map class** con el mapa estático utilizando un comando **map list**.

A continuación los parámetros opcionales de QoS que se pueden definir para un **map class**:

Define el **committed information rate** (CIR).

```
Router(config-map-class)# frame-relay cir {in | out} bps
```

Especifica el CIR de entrada o salida (**in** | **out**) en **bits** por segundo (bps) para un VC Frame Relay. El valor por defecto es 56000 bps. Ejemplo de uso:

```
frame-relay cir in  2000000
frame-relay cir out 9600
```

Define el mínimo aceptable para el CIR.

```
Router(config-map-class)# frame-relay mincir {in | out} bps
```

Especifica el CIR mínimo aceptable de entrada o salida (**in** | **out**) en **bits** por segundo (bps) para un VC Frame Relay. El valor por defecto es 56000 bps. La red utiliza el valor **mincir** cuando asigna los recursos para un VC. Si el valor del **mincir** no puede ser soportado, la conexión se libera.

Define el **Committed Burst Size** (Bc).

```
Router(config-map-class)# frame-relay bc {in | out} bits
```

Especifica el Bc de entrada o salida (**in** | **out**) en **bits** para un VC Frame Relay. Si no se especifica ningún valor, ambos son configurados. El rango de valores es de 300 hasta 16000000 y el valor por defecto es 7000 **bits**.

El Bc es especificado dentro de un **map class** para solicitar una cierta tasa de ráfaga para el circuito. Aunque está especificado en **bits**, un factor de tiempo implícito es el **time interval** (Tc), el cual esta definido como el **burst size** dividido por el CIR.

Define el **Excess Burst Size** (Be).

```
Router(config-map-class)# frame-relay be {in | out} bits
```

Especifica el Be de entrada o salida (**in** | **out**) en **bits** para un VC Frame Relay. El valor por defecto es 7000 **bits**.

Define la tasa de tráfico para la **map class**.

```
Router(config-map-class)# frame-relay traffic-rate average
[peak]
```

Configura todas las características del **traffic shaping** de un VC con un solo comando.

Descripción de los parámetros:

`average`. La tasa promedio en **bits** por segundos (bps), equivale a especificar el **committed information rate** (CIR) contratado.

`peak`. (Opcional) la tasa máxima (**peak rate**) en bps, equivalente a:

CIR + Be / Tc = CIR (1 + Be / Bc)

Si el valor `peak` no es configurado, la tasa máxima será el valor configurado para `average`.

Las tasas configuradas para `average` y `peak` son convertidas a los valores equivalentes de CIR, Be y Bc para uso del VC. Cuando los valores son traducidos, la tasa `average` es usada como el CIR. Este valor se asume que es para un segundo de tiempo. El valor Bc a generar es de 1/8 del CIR con un intervalo de 125 milisegundos.

El valor Be se deriva de la tasa `peak` al sustraer por la tasa `average`. El valor de la tasa `peak` menos el de la tasa `average` es asumido para ser de 1 segundo. El valor Be generado es 1/8 de la tasa `peak` menos la tasa `average` con un intervalo de 125 milisegundos. Si el valor `peak` no está configurado, la tasa máxima será por defecto el valor de `average` y el valor Be será igual a 0.

Por ejemplo, introducir el comando **frame-relay traffic-rate 64000 96000** resultará en un CIR de 64000 bps. Asumiendo 8 intervalos de 125 milisegundos, el Bc es 64000/8 u 8000 **bits**. El Be es calculado al sustraer 64000 de 96000, así que el valor de un segundo es 32000 **bits**. Para cada intervalo de 125 milisegundo, el valor Be es de 4000 **bits**.

Note que el comando **show frame-relay pvc** muestra los valores para Be y Bc basado en un intervalo de un segundo, pero internamente los valores usados están basados en un intervalo de 125 milisegundos.

El comando **frame-relay traffic-rate** permite configurar todas las características de **traffic shaping** de un circuito virtual en un solo comando. Usarlo es más simple que la alternativa de introducir los tres comandos **frame-relay cir out**, **frame-relay be out** y **frame-relay bc out**, pero ofrece un poco menos de flexibilidad.

Especifica una Lista de Colas de Prioridad.

```
Router(config-map-class)# frame-relay custom-queue-list list-
number
```

Asigna una **custom queue** al circuito virtual asociado con una **map class**.

Utilice además el comando **queue-list** para definir una **custom queue** (las tareas necesarias para su configuración se encuentran en el anexo C.). Si éste comando no es introducido, la cola por defecto es FIFO. Solo un tipo de cola puede ser asociado con un **map class** en particular, definiciones subsiguientes sobreescriben a las anteriores.

Ejemplo de uso:

```
queue-list 1 queue 4 byte-count 100

map-class frame-relay cust_vc
  frame-relay custom-queue-list 1

interface serial 0/0
  encapsulation frame-relay
  frame-relay interface-dlci 100
  class cust_vc
```

Especifica una Lista de Colas Configurables.

```
Router(config-map-class)# frame-relay priority-group list-
number
```

Asigna una **priority queue** al circuito virtual asociado con una **map class**.

Utilice además el comando **priority-list** para definir una **priority queue** (las tareas necesarias para su configuración se encuentran en el anexo C.). Si éste comando no es introducido, la cola por defecto es FIFO. Solo un tipo de cola puede ser asociado con un **map class** en particular, definiciones subsiguientes sobreescriben a las anteriores.

Ejemplo de uso:

```
priority-list 1 protocol ip high

map-class frame-relay pri_vc
  frame-relay priority-group 1

interface serial 0/0
  encapsulation frame-relay
  frame-relay interface-dlci 100
  class pri_vc
```

Selecciona BECN o **ForeSight** como mecanismo de notificación de congestión al cual se adaptará el **Traffic Shaping**.

```
Router(config-map-class)# frame-relay adaptive-shaping {becn |
foresight | interface-congestion [queue-depth]}
```

La función **ForeSight** en el **router** es la misma del **software** de Control de Tráfico de red usado en los **switches** Cisco y debe estar configurada

explícitamente en ambos dispositivos. Esta función permite a los **routers** Frame Relay Cisco procesar y reaccionar a los mensaje **ForeSight** y ajustar el **Traffic Shaping** a nivel de circuito virtual de una manera oportuna.

Cuando un **router** Cisco recibe un mensaje **ForeSight** indicando que un DLCI está experimentando congestión, éste reacciona activando su función de **Traffic Shaping** para reducir la tasa de salida. El **router** reacciona igual a como lo hubiera hecho si hubiera recibido un paquete con el **bit** BECN activado.

La diferencia entre los mecanismos de congestión BECN y **ForeSight**, es que el BECN requiere que se envíe un paquete en la dirección del DLCI congestionado para transmitir la señal. El envío de paquetes no es predecible y por consiguiente no es confiable como un mecanismo de notificación. En vez de esperar por los paquetes para proporcionar el mecanismo de notificación de congestión, los mensajes regulados del **ForeSight** garantizan que el **router** reciba la notificación antes que la congestión sea un problema. El tráfico puede ser reducido en la dirección del DLCI congestionado.

Descripción de los parámetros:

becn. Permite el ajuste de la tasa en respuesta a paquetes BECN.

foresight. Permite el ajuste de la tasa en respuesta a mensaje **ForeSight**.

interface-congestion. Permite el ajuste de la tasa en respuesta a congestión en la interfase.

Queue-depth. (Opcional) máximo número de paquetes que pueden estar en la cola de la interfase antes de que se considere que la interfase está congestionada. El rango es de 0 a 40 paquetes. Valor por defecto 0 paquetes.

Este comando reemplaza al comando **frame-relay becn-response-enable**.

El comando **frame-relay adaptive-shaping** configura un router para que ajuste la tasa de envío del circuito virtual en respuesta a mensajes de congestión BECN o **ForeSight**, o congestión en la interfase. Incluya este comando en una definición de **map class** y aplíquela a una interfaz o subinterfaz.

El **Traffic Shaping** adaptativo para congestión de interfases puede ser configurado junto a BECN o **ForeSight**. Cuando esto se hace, si la congestión de la interfases excede el parámetro **queue depth**, entonces la tasa de envío del VC es reducida al **minimum committed information rate** (minCIR). Cuando la congestión de la interfase cae debajo del **queue depth**, entonces la tasa de envío es ajustada en respuesta a BECN o **ForeSight**.

4.1.4 Configuraciones especiales

Las siguientes son configuraciones opcionales realizadas para personalizar una red Frame Relay:

- Configurar la lista **Discard Eligibility** (Opcional).
- Configurar los niveles de DLCI por prioridad (Opcional).

Configurar la lista Discard Eligibility[14]

Se puede especificar cuales paquetes Frame Relay tienen prioridad baja o ser sensibles al tiempo y ser los primeros en ser rechazados cuando un **switch** Frame Relay esté congestionado. El mecanismo que permite a un **switch** Frame Relay identificar tales paquetes es el **bit Discard Eligible** (DE).

Esta característica requiere que la red Frame Relay sea capaz de interpretar al **bit** DE. Algunas redes no realizan ninguna acción cuando el **bit** DE está establecido. Otras redes utilizan este **bit** para determinar cuales paquetes rechazar. La interpretación más deseable es usar el DE para determinar cuales paquetes deben ser rechazados primero y una sensibilidad al tiempo baja.

Se puede definir una lista que identifique las características de los paquetes a ser

14 Cisco Systems. Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2. Estados Unidos : Cisco Systems, 2001. Página WC-205.

elegidos para excluir, también se pueden especificar grupos DE para identificar el DLCI que es afectado.

Para definir una lista DE que especifique los paquetes que van a tener el **bit** DE ajustado y además puedan ser rechazados cuando el **switch** Frame Relay está congestionado, utilizar el siguiente comando en modo de configuración global:

```
Router(config)# frame-relay de-list list-number {protocol
protocol | interface type number} characteristic
```

Se pueden especificar listas DE basadas en el protocolo o interfase y en características como la fragmentación del paquete, puerto TCP o UDP, lista de acceso o tamaño del paquete.

Descripción de los parámetros:

`list-number`. Número de la lista DE.

protocol `protocol`. Uno de los siguientes valores que corresponde a los protocolos o dispositivos soportados:

arp	Address Resolution Protocol.
appletalk	AppleTalk.
bridge	bridging device.
clns	ISO Connectionless Network Service.
clns_es	CLNS end systems.
clns_is	CLNS intermediate systems.
compressedtcp	Compressed TCP.
decnet	DECnet.
decnet_node	DECnet end node.
decnet_router-L1	DECnet Level 1 (intra-area) router.
decnet_router-L2	DECnet Level 2 (interarea) router.
ip	Internet Protocol.
ipx	Novell Internet Packet Exchange Protocol.

`interface` `type`. Uno de los siguientes tipos: **serial**, **null**, o **ethernet**.

`number`. Número de la interfaz.

`characteristic`. Uno de los siguientes valores:

fragments	Fragmented IP packets
gt bytes	Sets the DE bit for packets larger than the specified number of bytes (including the 4-byte Frame Relay encapsulation).
list access-list-number	Previously defined access list number.
lt bytes	Sets the DE bit for packets smaller than the specified number of bytes (including the 4-byte Frame Relay encapsulation).
tcp port	TCP packets to or from a specified port.
udp port	User Datagram Protocol (UDP) packets to or from a specified port.

Para remover una lista DE entera, utilice la forma negada del comando sin parámetros u opciones.

La funcionalidad de prioridad requiere que la red Frame Relay sea capaz de interpretar el **bit** DE al indicar cuales paquetes pueden ser rechazados primero en caso de congestión o cuales son menos sensibles al tiempo o ambos. Cuando se calcule el tamaño del paquete, se debe incluir el tamaño del paquete de datos, el encabezado ICMP, encabezado IP y los **bytes** de encapsulación Frame Relay.

El siguiente ejemplo especifica que los paquetes IP mayores a 512 **bytes** (incluye los 4 bytes de la encapsulación Frame Relay) tendrán el **bit** DE fijado:

```
frame-relay de-list 1 protocol ip gt 512
```

Para definir un grupo DE que será usado con un DLCI específico, utilice el siguiente comando en modo de configuración de interfase:

```
Router(config-if)# frame-relay de-group group-number dlci
```

Descripción de los parámetros:

`group-number`. Número del grupo DE a aplicar a un DLCI específico. Rango de 1 a 10.

`dlci`. Número DLCI.

Para deshabilitar los números de grupo definidos, utilice la forma negada del comando sin parámetros.

Este comando requiere que Frame Relay este habilitado. La funcionalidad **DE group** es soportada solamente en el proceso de conmutación de paquetes.

Configurar los niveles de prioridad por DLCI[15]

Los niveles de prioridad por DLCI (**DLCI priority levels**) permiten separar diferentes tipos de tráfico y pueden proporcionar una herramienta de administración de tráfico para problemas de congestión causados por las

15 Cisco Systems. Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2. Estados Unidos : Cisco Systems, 2001. Página WC-206.

siguientes situaciones:

- Mezcla de tráfico interactivo y por lotes en el mismo DLCI.
- Colocación en colas del tráfico de sitios con velocidades de acceso alta en un destino con velocidad de acceso baja.

Antes de configurar los niveles de prioridad por DLCI, se deben realizar las siguientes tareas:

- Definir una lista de prioridad global (**global priority list**), como se indica en el anexo C (Requerido).
- Habilitar la encapsulación Frame Relay, ya explicado (Requerido).
- Definir un mapeo estático o dinámico de direcciones, ya explicado (Requerido).
- Asegurarse de definir cada uno de los DLCI a los cuales se les van a aplicar los niveles. Se pueden asociar los niveles de prioridad por DLCI a las subinterfases.
- Configurar la LMI, ya explicado (Opcional).

Los niveles de prioridad por DLCI proporcionan una forma para definir múltiples DLCI paralelos para diferentes tipos de tráfico. Estos niveles no asignan colas de prioridad dentro del **router** o **access server**; de hecho son independientes de los dispositivos de colas de prioridad. Sin embargo si se habilitan colas (**queueing**) y se usa el mismo DLCI para las colas, entonces los DLCI de alta prioridad pueden

ser puestos en las colas de alta prioridad.

Para configurar los niveles de prioridad por DLCI utilice el siguiente comando en modo de configuración de interfaz:

```
Router(config-if)# frame-relay priority-dlci-group
group_number high-dlci medium-dlci normal-dlci low-dlci
```

Descripción de los parámetros:

`group-number`. Especifica un número de grupo.

`high-dlci`. DLCI que tendrá el nivel de prioridad más alto.

`medium-dlci`. DLCI que tendrá el nivel de prioridad medio.

`normal-dlci`. DLCI que tendrá el nivel de prioridad normal.

`low-dlci`. DLCI que tendrá el nivel de prioridad más bajo.

Este comando permite definir diferentes DLCI para diferentes categorías de tráfico basado en prioridad de tráfico. Este comando por sí solo no define colas de prioridad, pero puede ser usado en conjunto con las colas de prioridad (**priority queueing**). Una lista de prioridad global debe ser definida y los DLCI asociados deben ser aplicados a la configuración antes de habilitar este comando. Asociar los DLCI a sus grupos potenciales y definir los niveles de prioridad. Este comando es usado para múltiples DLCI, donde los puntos de destino y origen son los mismos (rutas paralelas). Este

comando no debería ser usado en las interfases o subinterfases punto a punto, donde un solo DLCI es configurado. Un DLCI solo puede estar asociado con un grupo de prioridad; sin embargo, pueden haber múltiples grupos por interfase o subinterfase.

Se deben configurar los valores del DLCI para `high-dlci` y `medium-dlci`. Sí no se asocia explícitamente un DLCI a los niveles de prioridad `normal-dlci` y `low-dlci`, entonces el último DLCI especificado en la línea de comando es usado como el valor para los restantes parámetros. Por ejemplo, los siguientes dos comando son equivalentes:

```
frame-relay priority-dlci-group 1 40 50
frame-relay priority-dlci-group 1 40 50 50 50
```

Cuando se configuren entradas de mapeos estáticos usando el comando **frame-relay map** o al usar el protocolo **Inverse ARP**, el DLCI de alto nivel es el único DLCI que es mapeado. En el siguiente ejemplo, el DLCI 40 es definido con la más alta prioridad. Por consiguiente, el DLCI 40 es el único DLCI que debe ser incluido en el comando **frame-relay map** y el DLCI 50 no debe ser incluido.

```
interface serial 0/1
  ip address 192.168.10.1 255.255.255.0
  encapsulation frame-relay
  frame-relay priority-dlci-group 1 40 50 60 70
  frame-relay map ip 172.21.177.2 40 broadcast
```

4.1.5 Práctica 0: Consideraciones Iniciales

Hasta este punto ha llegado la "teoría" acerca de las configuraciones Frame Relay, de ahora en adelante se trabaja en su aplicación práctica sobre los **routers** para simular una red Frame Relay completa. Un método muy eficiente para estudiar las prácticas por primera vez, es el comparar la secuencia de comandos de cada práctica con los detalles sobre configuración dados anteriormente. A continuación se muestran los pasos iniciales para ejecutar las prácticas.

Iniciar routers sin configuraciones

Se deben iniciar los **routers** sin el archivo de configuración de inicio, para evitar que configuraciones anteriores interfieran con las nuevas. De forma que se deben utilizar los siguientes comandos en modo EXEC privilegiado, antes de realizar cualquier práctica:

Borrar el archivo de configuración inicial de la NVRAM:

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

Aparece la siguiente línea para confirmar el borrado:

```
Erasing the nvram filesystem will remove all files! Continue?
[confirm]
```

Para confirmar se presiona la tecla **ENTER**.

Reiniciar el **router**:

```
Router# reload
```

La siguiente línea aparece solo si se han hecho cambios a la configuración:

```
System configuration has been modified. Save? [yes/no]:
```

Como no se van a guardar los cambios realizados se escribe **n** y luego **ENTER**.

Aparece la siguiente línea para confirmar el reinicio:

```
Proceed with reload? [confirm]
```

Para la cual se presiona la tecla **ENTER**.

Luego, de unos tres minutos, que el **router** ha terminado la secuencia de inicio, éste pregunta si desea entrar en el modo de configuración inicial:

```
Would you like to enter the initial configuration dialog?
[yes/no]:
```

Para lo que se responde **n** y luego **ENTER**.

Conexión de los cables seriales

La interconexión de los **routers** a través de las WIC seriales, se realiza con los cables seriales DTE y DCE de acuerdo con los esquemas siguientes:

Figura 8 : Esquema de interconexión para 3 routers

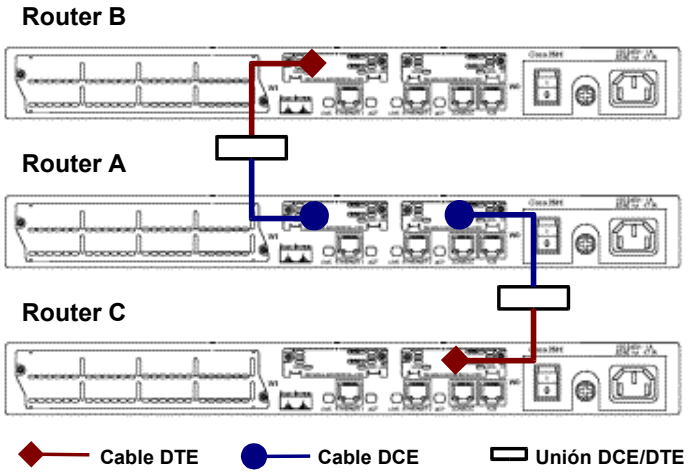
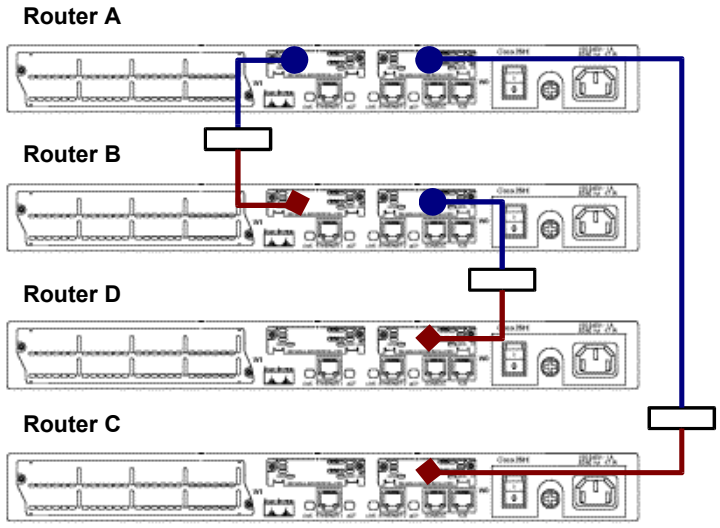


Figura 9 : Esquema de interconexión para 4 routers



Ejecución de la secuencia de comandos

Una de las formas más rápidas para cargar las configuraciones a cada **router** es utilizando el programa HyperTerminal.

Primero se conecta un cable de consola a uno de los puertos de comunicaciones seriales (COM 1 o COM 2) del computador y el otro extremo al puerto de consola del **router**. Luego se configuran los parámetros del puerto COM seleccionado, en HyperTerminal; así:

```
Bits por segundo      9600
Bits de datos         8
Paridad               Ninguno
Bits de parada        1
Control de flujo      Hardware
```

Una vez establecida la comunicación con el **router**, se siguen los pasos indicados anteriormente para “Iniciar **routers** sin configuraciones”.

Finalmente, se ingresa en el modo de configuración EXEC privilegiado; se copian (a partir de un archivo) las secuencias de comandos de las prácticas para cada **router** y se pegan en la ventana correspondiente en HyperTerminal, haciendo **click** derecho sobre ésta y pulsando el comando ”Pegar en el host”. Se repiten estos pasos con cada **router** hasta que se complete cada práctica.

Características especiales de Frame Relay[16]

Los apartados siguientes tratan sobre algunos comportamientos especiales del software IOS de Cisco con el protocolo Frame Relay.

Interfases Seriales

Las interfases seriales, que por defecto son multipunto, son medios de no **broadcast**, mientras que las subinterfases punto a punto sí permiten el **broadcast**. Si se utilizan las rutas estáticas, se puede apuntar al próximo salto o la subinterfase serial. Para multipunto se debe apuntar al próximo salto. Este concepto es muy importante cuando se utiliza el protocolo de enrutamiento OSPF sobre Frame Relay. El **router** necesita saber que esta interfaz soporta **broadcast** para que pueda trabajar OSPF.

Reconfigurar una subinterfaz

Una vez que se crea una subinterfaz con un tipo específico (**point-to-point** o **multipoint**) al cambiarlo, se debe reiniciar el **router**.

Realizar un Ping a la propia dirección IP

No es posible realizar un **ping** a la propia dirección IP en una (sub)interfases Frame Relay multipunto. Esto debido a que las interfases multipuntos no son

16 Cisco Systems. Comprehensive Guide to Configuring and Troubleshooting Frame Relay. Estados Unidos : Cisco Systems, 2003. Páginas 68 a 74.

broadcast, lo contrario a Ethernet y a las interfases punto a punto de HDLC y Frame Relay. Además no se puede realizar **ping** desde un **spoke** a otro **spoke** en una configuración **Hub & Spoke**. Esto es debido a que no hay mapeo para la IP propia (y ninguna se ha aprendido vía **Inverse ARP**). Pero si se configura un mapeo estático (usando el comando **frame-relay map**) para la IP propia (o una para el **spoke** remoto) para usar un DLCI local, entonces si se puede hacer **ping** al dispositivo.

Split Horizon

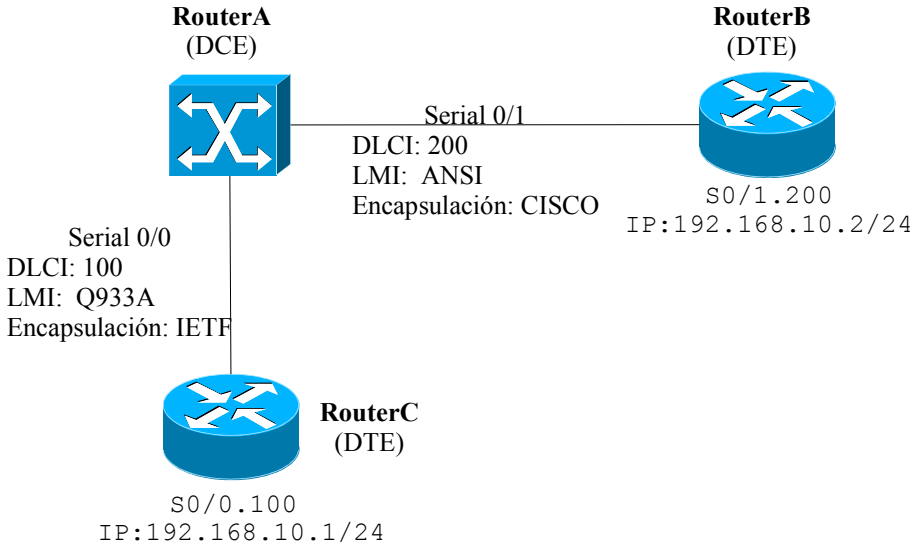
El chequeo del **split horizon** se deshabilita por defecto para la encapsulación Frame Relay, así que las actualizaciones de enrutamiento entran y salen por la misma interfaz. Algunos protocolos requieren que el **split horizon** esté habilitado, así que al configurar subinterfases Frame Relay se asegura que una interfaz física sea tratada como múltiples interfases virtuales. Los paquetes recibidos en una interfaz virtual pueden ser reenviados a otra interfaz virtual, aunque estén configurados en la misma interfaz física.

Keepalive

En algunos casos el **keepalive** del **router** Cisco necesita ser un poco más corto (aproximadamente de 8 segundos) que el del **switch**. Solo lo necesita si la interfaz fluctúa entre los estados **UP** y **DOWN**.

4.1.6 Práctica 1: Frame Relay Switching

Figura 10 : Esquema Frame Relay Switching



Objetivos

- Simular una red Frame Relay completa.
- Configurar el Router A para que simule un **switch** Frame Relay.
- Configurar los **routers** a los extremos del **switch** para permitir la comunicación a través de éste.
- Establecer distintos tipos de encapsulación y tipo de LMI en el **switch** para asignar una configuración con comandos explícitos en los **routers**.

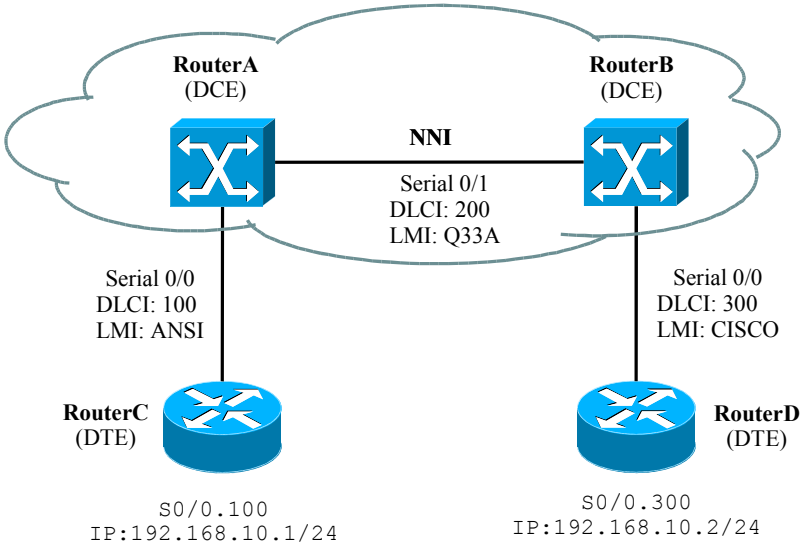
Secuencia de comandos

```
!RouterA (DCE)

config terminal
hostname RouterA

frame-relay switching


interface serial 0/0
  encapsulation frame-relay ietf
  frame-relay intf-type dce
  frame-relay lmi-type q933a
  frame-relay route 100 interface Serial 0/1 200
  clockrate 64000
  no shutdown
exit


interface serial 0/1
  encapsulation frame-relay
  frame-relay intf-type dce
  frame-relay lmi-type ansi
  frame-relay route 200 interface Serial 0/0 100
  clockrate 64000
  no shutdown
exit



!RouterB (DTE)

config terminal
hostname RouterB

interface serial 0/1
  encapsulation frame-relay
  frame-relay lmi-type ansi
  no shutdown

  interface serial 0/1.200 point-to-point
    ip address 192.168.10.2 255.255.255.0
    frame-relay interface-dlci 200
    exit
  exit
exit
```

```
!RouterC (DTE)

config terminal
hostname RouterC

interface serial 0/0
  encapsulation frame-relay ietf
  frame-relay lmi-type q933a
  no shutdown

  interface serial 0/0.100 point-to-point
    ip address 192.168.10.1 255.255.255.0
    frame-relay interface-dlci 100
    exit
  exit
exit
```

4.1.7 Práctica 2: Frame Relay NNI entre Switches

Figura 11 : Esquema Frame Relay NNI entre switches



Objetivos

- Simular una red Frame Relay completa.
- Configurar dos **routers** para que simulen ser **switches** Frame Relay.
- Simular las interconexiones de los **switches** de un proveedor de servicios (nube Frame Relay) al configurar los dos **switches** para soportar el protocolo **Network-to-Network Interface** (NNI).
- Configurar los **routers** en los extremos de la nube para permitir la comunicación a través de ésta.

Secuencia de comandos

!RouterA (DCE)

```
config terminal
hostname RouterA

frame-relay switching


interface serial 0/0
  no ip address
  encapsulation frame-relay
  frame-relay intf-type dce
  frame-relay lmi-type ansi
  frame-relay route 100 interface serial 0/1 200
  clockrate 64000
  no shutdown
exit


interface serial 0/1
  no ip address
  encapsulation frame-relay
  frame-relay intf-type nni
  frame-relay lmi-type q933a
  frame-relay route 200 interface serial 0/0 100
  clockrate 64000
  no shutdown
exit
```

!RouterB (DCE)

```
config terminal
hostname RouterB

frame-relay switching


interface serial 0/0
  no ip address
  encapsulation frame-relay
  frame-relay intf-type dce
  !(LMI Autosense)
  frame-relay route 300 interface serial 0/1 200
  clockrate 64000
  no shutdown
exit


interface serial 0/1
  no ip address
```

```
  encapsulation frame-relay
  frame-relay intf-type nni
  frame-relay lmi-type q933a
  frame-relay route 200 interface serial 0/0 300
 !
  no shutdown
exit
```

!RouterC (DTE)

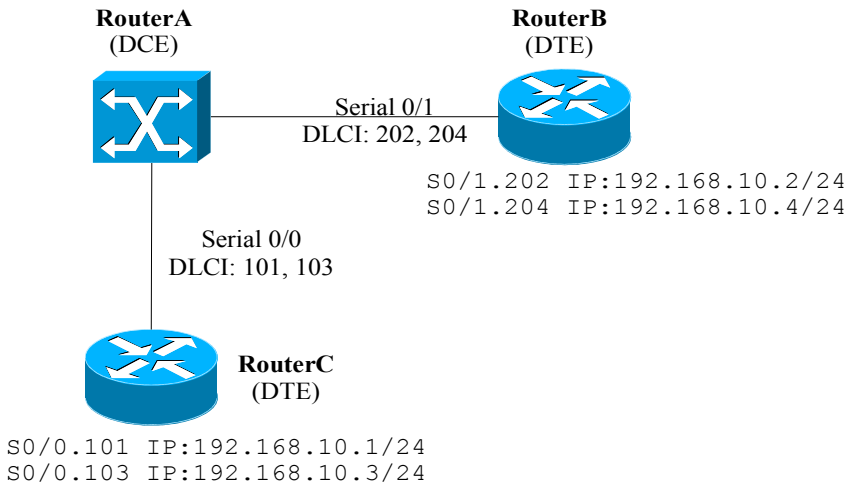
```
config terminal
hostname RouterC


interface serial 0/0
  encapsulation frame-relay
  frame-relay intf-type dte
  frame-relay lmi-type ansi

  no shutdown

  interface serial 0/0.100 point-to-point
    ip address 192.168.10.1 255.255.255.0
    frame-relay interface-dlci 100
    exit
  exit
exit
```

!RouterD (DTE)

```
config terminal
hostname RouterD


interface serial 0/0
  encapsulation frame-relay
  !(Valor por defecto DTE)
  !(LMI Autosense)

  no shutdown

  interface serial 0/0.300 point-to-point
    ip address 192.168.10.2 255.255.255.0
    frame-relay interface-dlci 300
    exit
  exit
exit
```

4.1.8 Práctica 3: Frame Relay Traffic Shaping

Figura 12 : Esquema Frame Relay Traffic Shaping



Objetivos

- Simular una red Frame Relay completa.
- Configurar el Router A para que simule un **switch** Frame Relay.
- Configurar el Router C para que emplee **Frame Relay Traffic Shaping**, con dos **map class**; aplicando cada clase en un DLCI distinto.

Secuencia de comandos

```
!RouterA (DCE)

config terminal
hostname RouterA

frame-relay switching


interface Serial 0/0
  no ip address
  encapsulation frame-relay
  frame-relay intf-type dce
  frame-relay lmi-type cisco

  frame-relay route 101 interface Serial 0/1 202
  frame-relay route 103 interface Serial 0/1 204

  clockrate 64000
  no shutdown
exit


interface Serial 0/1
  no ip address
  encapsulation frame-relay
  frame-relay intf-type dce
  frame-relay lmi-type cisco

  frame-relay route 202 interface Serial 0/0 101
  frame-relay route 204 interface Serial 0/0 103

  clockrate 64000
  no shutdown
exit



!RouterB (DTE)

config terminal
hostname RouterB


interface serial 0/1
  encapsulation frame-relay
  no shutdown

  interface serial 0/1.202 point-to-point
    ip address 192.168.10.2 255.255.255.0
```

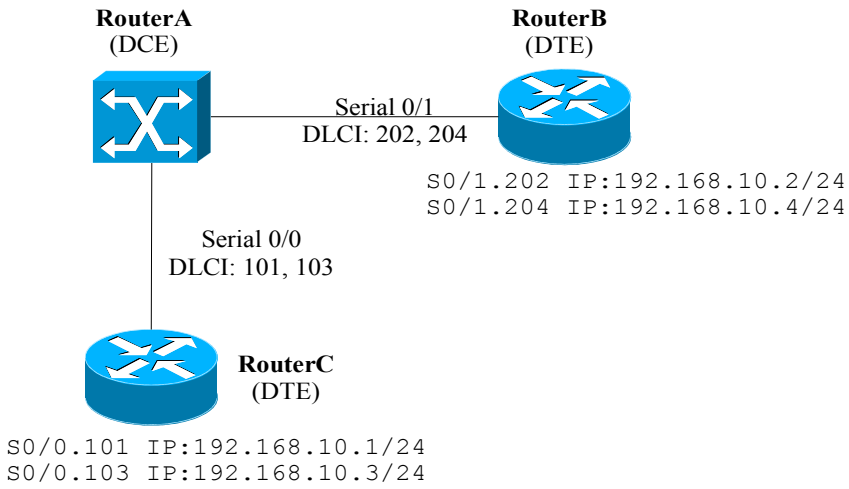
```
    frame-relay interface-dlci 202
    exit
  exit

  interface serial 0/1.204 point-to-point
    ip address 192.168.10.4 255.255.255.0
    frame-relay interface-dlci 204
    exit
  exit

exit
```

!RouterC (DTE)

```
config terminal
hostname RouterC


map-class frame-relay clase_slow
  frame-relay traffic-rate 9600 12000
exit

map-class frame-relay clase_fast
  frame-relay traffic-rate 16000 64000
exit


interface Serial 0/0
  no ip address
  encapsulation frame-relay
  frame-relay traffic-shaping
  no shutdown

  interface Serial 0/0.101 point-to-point
    ip address 192.168.10.1 255.255.255.0
    frame-relay class clase_fast
    frame-relay interface-dlci 101
    exit

  interface Serial 0/0.103 point-to-point
    ip address 192.168.10.3 255.255.255.0
    frame-relay class clase_slow
    frame-relay interface-dlci 103
    exit

exit
```

4.1.9 Práctica 4: Frame Relay Traffic Shaping con Colas

Figura 13 : Esquema Frame Relay Traffic Shaping con Colas



Objetivos

- Simular una red Frame Relay completa.
- Configurar el Router A para que simule un **switch** Frame Relay.
- Configurar el Router B para que emplee **Frame Relay Traffic Shaping** con colas configurables y colas por prioridad.

Secuencia de comandos

```
!RouterA (DCE)

config terminal
hostname RouterA

frame-relay switching


interface Serial 0/0
  no ip address
  encapsulation frame-relay
  frame-relay intf-type dce
  frame-relay lmi-type cisco

  frame-relay route 101 interface Serial 0/1 202
  frame-relay route 103 interface Serial 0/1 204

  clockrate 64000
  no shutdown
exit


interface Serial 0/1
  no ip address
  encapsulation frame-relay
  frame-relay intf-type dce
  frame-relay lmi-type cisco

  frame-relay route 202 interface Serial 0/0 101
  frame-relay route 204 interface Serial 0/0 103

  clockrate 64000
  no shutdown
exit
```

```
!RouterB (DTE)

config terminal
hostname RouterB


!Configurar Custom Queueing
access-list 100 permit tcp any any eq 2065
access-list 115 permit tcp any any eq 256

queue-list 1 protocol ip 1 list 100
queue-list 1 protocol ip 2 list 115
queue-list 1 default 3

queue-list 1 queue 1 byte-count 1600 limit 200
queue-list 1 queue 2 byte-count 600  limit 200
queue-list 1 queue 3 byte-count 500  limit 200


!Configurar Priority Queueing
priority-list 2 protocol ip high
priority-list 2 protocol ip medium tcp telnet
priority-list 2 default normal


!Aplicar las colas a los map class
map-class frame-relay clase_slow
  frame-relay traffic-rate 4800 9600
  frame-relay custom-queue-list 1
  frame-relay adaptive-shaping becn
exit

map-class frame-relay clase_fast
  frame-relay traffic-rate 16000 64000
  frame-relay priority-group 2
  frame-relay adaptive-shaping becn
exit


interface serial 0/1
  no ip address
  encapsulation frame-relay
  frame-relay traffic-shaping
  frame-relay class clase_slow
  no shutdown

  interface serial 0/1.202 point-to-point
    ip address 192.168.10.2 255.255.255.0
    frame-relay interface-dlci 202
    exit

  interface serial 0/1.204 point-to-point
    ip address 192.168.10.4 255.255.255.0
    frame-relay interface-dlci 204
      class clase_fast
    exit
```

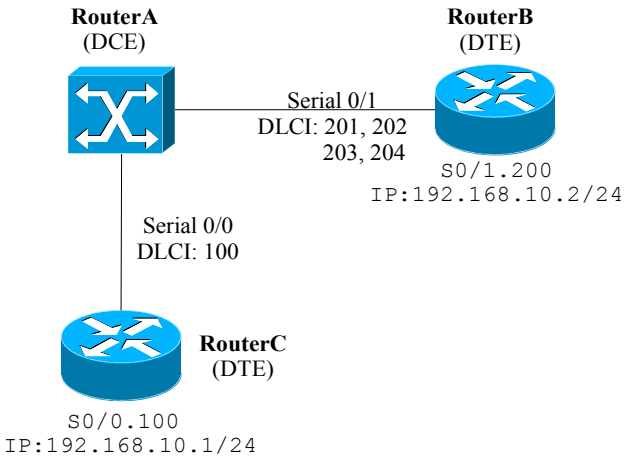
```
exit
```

!RouterC (DTE)

```
config terminal
hostname RouterC


interface serial 0/0
  encapsulation frame-relay
  no shutdown

  interface serial 0/0.101 point-to-point
    ip address 192.168.10.1 255.255.255.0
    frame-relay interface-dlci 101
    exit
  exit

  interface serial 0/0.103 point-to-point
    ip address 192.168.10.1 255.255.255.0
    frame-relay interface-dlci 103
    exit
  exit

exit
```

4.1.10 Práctica 5: Frame Relay con prioridad por DLCI

Figura 14 : Esquema Frame Relay prioridad por DLCI



Objetivos

- Simular una red Frame Relay completa.
- Configurar el Router A para que simule un **switch** Frame Relay.
- Configurar el Router B para que emplee prioridad por DLCI.

Secuencia de comandos

```
!RouterA (DCE)

config terminal
hostname RouterA

frame-relay switching


interface Serial 0/0
  no ip address
  encapsulation frame-relay
  frame-relay intf-type dce
  frame-relay lmi-type cisco

  frame-relay route 100 interface Serial 0/1 201

  clockrate 64000
  no shutdown
exit

interface Serial 0/1
  no ip address
  encapsulation frame-relay
  frame-relay intf-type dce
  frame-relay lmi-type cisco

  frame-relay route 201 interface Serial 0/0 100
  frame-relay route 202 interface Serial 0/0 100
  frame-relay route 203 interface Serial 0/0 100
  frame-relay route 204 interface Serial 0/0 100

  clockrate 64000
  no shutdown
exit
```

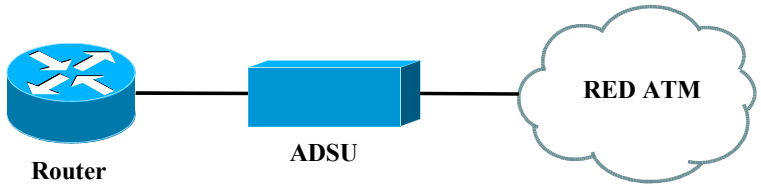
```
!RouterB (DTE)

config terminal
hostname RouterB


access-list 102 permit icmp any any

priority-list 1 protocol ip high   list 102
priority-list 1 protocol ip medium tcp telnet
priority-list 1 protocol ip normal tcp ftp
priority-list 1 protocol ip low


interface serial 0/1
  no ip address
  encapsulation frame-relay
  no shutdown
  priority-group 1

  interface serial 0/1.200 multipoint
    ip address 192.168.10.2 255.255.255.0
    frame-relay priority-dlci-group 1 201 202 203 204
    frame-relay interface-dlci 201
    exit
  exit
exit



!RouterC (DTE)

config terminal
hostname RouterC


interface serial 0/0
  no ip address
  encapsulation frame-relay
  no shutdown

  interface serial 0/0.100 multipoint
    ip address 192.168.10.1 255.255.255.0
    frame-relay interface-dlci 100
    exit
  exit
exit
```

4.2 PROTOCOLO ATM

Configuración del acceso ATM sobre una interfaz serial[17]

Esta sección describe como configurar **routers** que utilizan una interfaz serial para tener acceso ATM a través de un **ATM data service unit** (ADSU), como se ilustra en la figura 15. La lista de tareas incluye los pasos necesarios para habilitar la encapsulación **Asynchronous Transfer Mode-Data Exchange Interface** (ATM-DXI).

Figura 15 : Configuración ATM típica



En **routers** con una interfaz serial, un ADSU es requerido para proveer la interfaz ATM hacia la red, convirtiendo los paquetes de salida en celdas ATM y rearmando las celdas entrantes en paquetes.

Cualquier interfaz serial puede ser configurada para la encapsulación

17 Cisco Systems. Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2. Estados Unidos : Cisco Systems, 2001. Páginas WC-93 a WC-95.

multiprotocolo sobre ATM-DXI, como lo especifica el RFC 1483. En la ADSU, la cabecera DXI es removida y los datos del protocolo son segmentados dentro de celdas para su transporte sobre la red ATM.

El RFC 1483 describe dos formas para transportar tráfico multiprotocolo que interconecta redes no orientadas a la conexión sobre una red ATM. Un método permite la multiplexación de varios protocolos sobre un solo PVC. El otro método usa diferentes circuitos virtuales para transportar los diferentes protocolos. La implementación de Cisco del RFC 1483 soporta ambos métodos y el soporte de tráfico para los protocolos: Apollo Domain, AppleTalk, Banyan VINES, DECnet, IP, Novell IPX, ISO CLNS y XNS.

Lista de tareas

Para configurar el acceso ATM sobre una interfaz serial se deben realizar las siguientes tareas. Cada tarea es identificada como requerida u opcional.

- Habilitar la interfaz serial (Requerida).
- Habilitar la encapsulación ATM-DXI (Requerida).
- Configurar el PVC para el ATM-DXI (Requerida).
- Mapeo de la dirección del protocolo para el PVC del ATM-DXI (Requerida).
- Monitoreo y mantenimiento de la interfaz serial ATM-DXI (Opcional).

Habilitar la interfaz serial

Para configurar la interfaz serial para acceso ATM, habilite la interfaz serial usando los siguientes comandos comenzando en el modo de configuración global:

```
Router(config)# interface serial number
Router(config-if)# ip address address mask
```

Habilitar la encapsulación ATM-DXI

Para habilitar la encapsulación ATM-DXI en una interfaz serial o **High-Speed Serial Interface** (HSSI), utilice el siguiente comando en modo de configuración de interfaz:

```
Router(config-if)# encapsulation atm-dxi
```

Configurar el PVC para el ATM-DXI

Un PVC de ATM-DXI puede ser definido para transportar uno o más protocolos como lo describe el RFC 1483 o múltiples protocolos como lo describe el RFC 1490.

Para configurar un PVC de ATM-DXI y seleccionar un método de encapsulación, utilice el siguiente comando en modo de configuración de interfaz:

```
Router(config-if)# dxi pvc vpi vci [snap | nlpid | mux]
```

La opción **multiplex** (MUX) define que el PVC transportará solo un

protocolo, cada protocolo debe ser transportado en un PVC diferente. La opción **Subnetwork Access Protocol** (SNAP) es una encapsulación multiprotocolo LLC/SNAP, compatible con el RFC 1483; SNAP es la opción por defecto. La opción **network layer protocol identification** (NLPID) es una encapsulación multiprotocolo, compatible con el RFC 1490; esta opción es provista para tener compatibilidad hacia atrás con la configuración por defecto en las primeras versiones del Cisco IOS.

Mapeo de la dirección del protocolo para el PVC del ATM-DXI

Describe como realizar el mapeo de una dirección de protocolo al VCI y VPI de un PVC que puede transportar tráfico multiprotocolo. La dirección de protocolo pertenece al **host** en el otro extremo del enlace. Para mapear una dirección de protocolo a un PVC del ATM-DXI, utilice el siguiente comando en modo de configuración de interfase:

```
Router(config-if)# dxi map protocol protocol-address vpi vci
[broadcast]
```

Repetir esta tarea por cada protocolo que sea transportado por el PVC. Los protocolos soportados son: Apollo Domain, AppleTalk, Banyan VINES, DECnet, IP, Novell IPX, ISO CLNS, y XNS.

Monitoreo y mantenimiento de la interfaz serial ATM-DXI

Mostrar información de estado de la interfaz ATM serial.

```
Router# show interfaces atm [slot/port]
```

Mostrar información del PVC en ATM-DXI.

```
Router# show dxi pvc
```

Mostrar información del mapeo ATM-DXI.

```
Router# show dxi map
```

Ejemplo de acceso ATM sobre una interfaz serial

La interfaz **serial interface 0/0** será configurada para ATM-DXI con encapsulación MUX. Debido a que la encapsulación MUX es usada, solo un protocolo es transportado en el PVC. Este protocolo está explícitamente identificado por un comando **dxi map**, el cual identifica también la dirección de protocolo del nodo remoto. Este PVC puede transportar tráfico de **broadcast** IP.

```
interface serial 0/0
  ip address 172.21.178.48
  encapsulation atm-dxi
  dxi pvc 10 10 mux
  dxi map ip 172.21.178.4 10 10 broadcast
```

4.3 PROTOCOLO RDSI/ISDN

Desafortunadamente no se pueden realizar configuraciones del protocolo RDSI sobre interfases seriales. Estas deben realizarse sobre interfases ISDN BRI, ISDN PRI o T1/E1.

CONCLUSIONES

Se realizó una amplía recopilación y documentación de las técnicas de gestión del ancho de banda en la WAN, que por limitaciones en el tamaño del documento impreso no se han incluido en éste; pero se pueden encontrar en el documento complementario dentro del CD-ROM adjunto.

La información expuesta acerca de las distintas técnicas de gestión es, a pesar de su extensión, solo una introducción donde se dan a conocer las principales características de cada una de ellas. En el desarrollo de las diversas técnicas han invertido años de trabajo decenas de personas altamente calificadas; lo que resulta en la existencia de especificaciones y estándares muy detallados, interrelacionados y extensos, mantenidos por los mismos grupos de trabajo donde se desarrollaron.

Las capacidades para WAN de la familia de **routers** Cisco 2600 se han determinado en relación a las características de los protocolos WAN que pueden soportar basados en estándares internacionales y extensiones propias de Cisco incorporados en su sistema operativo IOS y en la variedad de módulos hardware

opcionales que se pueden agregar a estos **routers** para permitir la implementación de una tecnología WAN determinada.

Se documentó de forma detallada los pasos necesarios para la simulación o emulación de una red completa para un protocolo WAN determinado. Esta red incluye la configuración de los dispositivos del proveedor de servicio y del usuario. Con las configuraciones actuales de los **routers** de la UTB, el **software** Cisco IOS permite simular de forma completa el protocolo Frame Relay y la configuración del lado del usuario para ATM; que son los protocolos a los cuales se encaminó realizar la simulación por ser los más implementados en nuestro entorno (Colombia).

Se implementaron varias prácticas de ejemplo que simulan de forma completa el protocolo Frame Relay. Estas prácticas de laboratorio ilustran una secuencia de comandos que permiten alcanzar unos objetivos específicos planteados para cada práctica de laboratorio. Así mismo estas prácticas enriquecen en calidad y número a las ya disponibles para las personas que realizan los cursos del CCNA.

De forma general en las interfases seriales se puede aplicar cualquier técnica de gestión del ancho de banda de las que se detallan en la guía “Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.3”. En ésta se explica de forma específica como implementar con el **software** IOS varios grupos de técnicas, las

cuales tienen restricciones de uso y protocolos para los que están optimizadas. Desarrollar prácticas para cada una de ellas es viable para varios trabajos monográficos bien coordinados y delimitados, teniendo presente las limitaciones en equipos del laboratorio de redes de la UTB y las mismas técnicas.

Se detalló cómo realizar la configuración del **Frame Relay Traffic Shaping**, que es una técnica de gestión del ancho de banda adaptada especialmente a las características de conmutación del protocolo Frame Relay. En su implementación pueden utilizarse de forma opcional listas de colas configurables o listas de colas por prioridad para elegir qué tipo de paquetes se van a tratar de forma preferencial.

RECOMENDACIONES

La documentación de las técnicas de gestión del ancho de banda en la WAN, debe verse como un esfuerzo para señalar las principales características de un grupo de técnicas representativas y un medio para conocer acerca de la evolución histórica de éstas, mediante la descripción del problema de red que cada técnica busca solucionar. Esto último sabiendo que el problema en la red depende de factores cómo el número de usuarios, tipo de aplicaciones utilizadas, calidad y capacidad del medio de comunicación, etc. Todas éstas, variables cuya magnitud han sufrido y sufren cambios con los años.

Las prácticas de laboratorio para protocolos WAN se realizaron para que pudieran ejecutarse con las configuraciones de los **routers** disponibles, que solo cuentan con dos interfases seriales. Esto redujo el número de prácticas que se implementaron; incluyendo al mismo protocolo Frame Relay, el cual es el único que puede ser simulado completamente en los **routers** Cisco 2600. Por lo tanto todavía quedan varias configuraciones que se pueden implementar para Frame Relay como lo es la configuración **Hub & Spoke** donde se requiere que el **router** que actúa como **switch** se conecte físicamente con otros tres **routers**, por lo que

se necesitan en éste **router** tres interfases seriales. Por esto en la medida en que se vayan adquiriendo interfases adicionales para los **routers** (seriales, ATM o RDSI) y los **switches** necesarios u otros dispositivos que los simulen, como el **switch** ADTRAN Atlas 550, se deben desarrollar las simulaciones o implementaciones reales de los protocolos WAN más usados en nuestro medio (ATM, RDSI o Frame Relay).

Las explicaciones de las configuraciones se realizaron utilizando como base la documentación más actual para el IOS, la versión 12.3, la cual no difiere en mucho con la versión 12.1 que utilizan los **routers** de la Universidad Tecnológica de Bolívar. La mayor diferencia que se puede encontrar es en la adición de parámetros para comandos de verificación (como **show**). Las secuencias de comandos de las prácticas de laboratorio solo han sido probadas en los **routers** de la UTB, así que se recomienda verificar los comandos si su versión de IOS es diferente a la 12.1.

Las prácticas donde se utiliza **Frame Relay Traffic Shaping** y **Frame Relay Traffic Shaping** con colas; buscan ilustrar cómo un fabricante, en nuestro caso Cisco, implementa una técnica de gestión del ancho de banda. Las técnicas de colas por prioridad y colas configurables se pueden aplicar a todo tipo de interfaz y protocolo, teniendo presente sus recomendaciones y restricciones de uso.

Se ha usado la frase “simular un protocolo WAN” porque eso es lo que puede alcanzarse con los dispositivos y configuraciones actuales del laboratorio de redes, y limitado a Frame Relay.

Incentivar a los estudiantes a tratar en próximos proyectos de monografías, el estudio de una técnica de gestión del ancho de banda en especial, de manera que se investigue a profundidad en sus especificaciones y estándares, e incluso se realice su implementación con los recursos con que cuenta el laboratorio de redes de la Universidad Tecnológica de Bolívar.

Antes de iniciar trabajos más profundos sobre protocolos WAN se debería investigar y dejar constancia de cómo funcionan los principales protocolos que permiten la conmutación en RDSI, Frame Relay y ATM; como son NNI, UNI y PNNI, que sobresalen entre otros. Para llevarlo a cabo se deben realizar estos trabajos con un buen apoyo de los participantes, ya que el conseguir los documentos con las especificaciones y estándares puede ser difícil en algunos casos, pero sobre todo extensos en la lectura.

BIBLIOGRAFÍA

SHELDON, Tom. Encyclopedia of Networking and Telecommunications. Estados Unidos : McGraw-Hill, 2001. 1447 p. ISBN 0072120053.

Cisco Systems. Internetworking Technology Handbook. Estados Unidos : Cisco Systems, 2003. Disponible en: www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ index.htm

Cisco Systems. Internetwork Design Guide. Estados Unidos : Cisco Systems, 2003. Disponible en: www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/ index.htm

Cisco Systems. Comprehensive Guide to Configuring and Troubleshooting Frame Relay. Estados Unidos, Cisco Systems, 2003. 78 p. Disponible en: www.cisco.com/en/US/tech/tk713/tk237/technologies_tech_note09186a008014f8 a7.shtml y www. cisco.com/warp/public/125/12.pdf.

Cisco Systems. Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2. Estados Unidos : Cisco Systems, 2001. 422 p. Disponible en: www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/wan_vcg.pdf.

Cisco Systems. Cisco IOS Wide-Area Networking Command Reference, Release 12.3. Estados Unidos : Cisco Systems, 2003. 867 p. Disponible en: www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/wan_r/wrgbook.pdf

Cisco Systems. Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.3. Estados Unidos : Cisco Systems, 2001. 478 p. Disponible en: www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/qos_vcg.pdf.

Cisco Systems. Cisco IOS Quality of Service Solutions Command Reference, Release 12.3. Estados Unidos : Cisco Systems, 2003. 474 p. Disponible en: www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/qos_r/qosbook.pdf.

Cisco Systems. Cisco IOS Dial Technologies Configuration Guide, Release 12.3. Estados Unidos : Cisco Systems, 2003. 962 p. Disponible en: www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/dial_vcg.pdf.

ATM Forum Europa. ATM in Europe: The User Handbook. Bélgica : ATM Forum, 1997. 79 p. Disponible en: www.atmforum.com/aboutatm/handbook.html.

ATM Forum Technical Committee. ATM Forum Addressing: Reference Guide. AF-RA-0106.000. Estados Unidos : ATM Forum, 1999. 48 p. Disponible en: ftp://ftp.atmforum.com/pub/approved-specs/af-ra-010%0A6.000.pdf.

ATM Forum Technical Committee. Private Network-Network Interface, Specification Version 1.1. AF-PNNI-0055.002. Estados Unidos : ATM Forum, 2002. 536 p. Disponible en: ftp://ftp.atmforum.com/pub/appr%0Aoved-specs/af-pnni-0055.002.pdf.

ATM Forum Technical Committee. ATM User-Network Interwork Interface (UNI) Specification Version 4.1. AF-ARCH-0193.000. Estados Unidos : ATM Forum, 2002. 9 p. Disponible en: ftp://ftp.atmforum.com/pub/approved-specs/af-arch-0193.000.pdf.

FLORES PÉREZ, Guido Fidel. Características de los Equipos ATM y su respuesta ante Tráfico Multimedia. Méjico. 1996. Disponible en: www.upaep.mx/puebla/atm/.

HINDIN, Eric. Say what? QoS in English. Network World Fusion. (Agosto, 1998). Disponible en: www.itworld.com/Net/4009/NWW980817QoS/pfindex.html

HOOVER, Mark. Class Of Marketing. Hoov's Musings. Vol. 1, No. 3. Disponible en: www.acuitive.com/musings/hmv1-3.htm

KARTALOPOULOS, Stamatios V. Understanding SONET/SDH and ATM : communications networks for the next millennium. Estados Unidos : IEEE Press, 1999. 257 p. IEEE Press understanding science & technology. ISBN 0-7803-4745-5.

FEIT, Sidnie. Wide Area high speed networks. MTP, 1999. 598 p. Macmillan Network Architecture and Development Series. ISBN 1-57870-114-7.

PAQUET, Catherine y TEARE, Diane. Creación de redes Cisco escalables. España : Pearson Educación, 2001. 772 p. ISBN 84-205-3185-5.

CHAPPELL, Laura. Advanced Cisco Router configuration. Estados Unidos : Cisco Press, 1999. 644 p. ISBN 1-57870-074-4.

COULIBALY, Mack M. Cisco IOS Releases: The complete reference. Estados Unidos : Cisco Press, 2000. 308 p. ISBN 1-57870-179-1.

LEINWAND, Allan y PINSKY, Bruce. Configuración de Routers Cisco. 2 ed. España : Pearson Educación, 2001. 376 p. ISBN 84-205-3188-5.

ANEXOS

ANEXO A. LISTA DE ACRÓNIMOS

AAL	ATM Adaptation Layer
ABR	Available Bit Rate
ACTS	Advanced Communications Technologies and Services
API	Application Program Interface
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
B-ICI	B-ISDN Inter Carrier Interface
B-ISDN	Broadband-ISDN
BUS	Broadcast and Unknown Server
CATV	Cable TV
CBDS	Connectionless Broadband Data Service
CBR	Constant Bit Rate
CDV	Cell Delay Variation
CEC	Commission of the European Community
CES	Circuit Emulation Services
CLNAP	ConnectionLess Network Access Protocol
CLP	Cell Loss Priority
CLR	Cell Loss Ratio
CMIP	Common Management Interface Protocol
CNM	Customer Network Management
CS	Convergence sublayer
CSCW	Computer Supported Collaborative Work

CTD	Cell Transfer Delay
ELAN	Emulated LAN
ETSI	European Telecommunications Standard Institute
FDDI	Fibre Distributed Data Interface
FR	Frame Relay
FTP	File Transfer Protocol
FUNI	Frame based UNI
GCRA	Generic Cell Rate Algorithm
HEC	Header Error Control
HTML	HyperText Markup Language
IISP	Interim inter-switch signaling protocol
ILMI	Interim Local Management Interface
IP	Internet Protocol
IPV6	Internet Protocol, version 6
IPX	Internetwork Packet Exchange
ISDN	Integrated Services Digital Network
IT	Information Technology
ITU	International Telecommunication Union
LAN	Local Area Network
LANE	LAN Emulation
LEC	LAN Emulation Client
LECS	LAN Emulation Configuration Server
LES	LAN Emulation Server
LUNI	LAN Emulation UNI
MAC	Media Access Control
MAN	Metropolitan area networks
MBS	Maximum Burst Size

MCR	Minimum Cell Rate
MIB	Management Information Base
MPEG	Motion Picture Experts Group
MPOA	MultiProtocol Over ATM
MSS	MAN Switching System
N-ISDN	Narrowband-ISDN
NNI	Network Node Interface
nrt-VBR	non real time VBR
OAM	Operation Administration and Maintenance
ONP	Open Network Provision
OS	Operation System
OSI	Open Systems Interconntection
PCR	Peak Cell Rate
PDH	Plesiochronous Digital Hierarchy
PICS	Protocol Implementation Conformance Statement
PM	Physical Medium
PNNI	Private NNI
PNO	Public Network Operator
PSTN	Public Switched Telephone Network
PT	Payload Type
PTO	Public Telephone Operator
PVC	Permanent Virtual Channel
QoS	Quality of Service
rt-VBR	real time VBR
SAR	Segmentation and Reassembly sublayer
SCR	Sustainable Cell Rate
SDH	Synchronous Digital Hierarchy

SEAL	Simple and Efficient Adaptation Layer
SMDS	Switched Multi-megabit Data Service
SMTP	Simple Mail Transfer Protocol
STM	Synchronous Transfer Mode
SVC	Switched Virtual Channel
TC	Transmission Convergence
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	Time Division Multiplexing
TIP	Transport and Interworking Package
TMN	Telecommunications Management Network
UBR	Unspecified Bit Rate
UNI	User Network Interface
UPC	Usage Parameter Contol
VBR	Variable Bit Rate
VCC	Virtual Channel Connection
VCI	Virtual Channel Identifier
VCL	Virtual Channel Link
VLAN	Virtual LAN
VOD	Video-On-Demand
VP	Virtual Path
VPI	Virtual Path Identifier
VPN	Virtual Private Network
WAIS	Wide Area Information Service
WAN	Wide Area Network
WWW	World Wide Web

ANEXO B. POLICING Y SHAPING APLICADO POR CISCO IOS

NOTA: por motivos de espacio no se pudo incluir este anexo en la documentación impresa, pero puede encontrarlo en toda su extensión en el documento complementario que se encuentra en el CD-ROM adjunto.

ANEXO C. QOS CON COLAS APLICADO POR CISCO IOS

NOTA: por motivos de espacio no se pudo incluir este anexo en la documentación impresa, pero puede encontrarlo en toda su extensión en el documento complementario que se encuentra en el CD-ROM adjunto.

ANEXO D. TARJETAS DE EXPANSIÓN EN ROUTERS CISCO 2600

A continuación se presentan los distintos módulos que pueden ser instalados en las correspondientes ranuras de los **routers** Cisco 2600, la información está disponible en el documento “Cisco 2600 Series Modular Access Routers” en el URL: www.cisco.com/warp/public/cc/pd/rt/2600/prodlit/2600_ds.pdf

TARJETAS DE INTERFAZ WAN (WIC)

Voice Interface Cards (VIC) para ser usadas con Voice/Fax Network Modules

Product Number	Description	2612	2600XM	2691
VIC-2BRI-S/T-TE	2-port BRI S/T Terminal Equipment Voice/Fax Interface Card for Voice/Fax NM	X	X	X
VIC-2BRI-NT/TE	2-port BRI (NT and TE) Voice Interface Module	X	X	X
VIC2-2BRI-NT/TE	2-port BRI (NT and TE) Voice Interface Module		X	X
VIC-2FXS	2-port FXS Voice/Fax Interface Card for Voice/Fax NM	X	X	X
VIC2-2FXS	2-port Voice Interface Card—FXS		X	X
VIC-4FXS/DID	4-port FXS Voice/Fax Interface Card. (Note: The DID feature is not supported at this time.)		X	X
VIC-2FXO-M1	2-port FXO Voice/Fax Interface Card for Voice/Fax NM with Caller ID & Supervisory Disconnect (North American version and other countries)	X	X	X
VIC-2FXO	2-port FXO Voice/Fax Interface Card for Voice/Fax Network module (North American version and other countries)	X	X	X
VIC2-2FXO	2-port Voice Interface Card—FXO (Universal)		X	X
VIC2-4FXO	4-port Voice Interface Card—FXO (Universal)		X	X
VIC-2FXO-M2	2-port FXO Voice/Fax Interface Card with Caller ID and Supervisory Disconnect (Europe version)	X	X	X
VIC-2FXO-EU	2-port FXO Voice/Fax Interface Card (Europe version)	X	X	X
VIC-2FXO-M3	2-port FXO Voice/Fax Interface Card for Australia	X	X	X
VIC-2DID	2-port DID (Direct Inward Dial) Voice/Fax Interface Card	X	X	X
VIC-2CAMA	2-port CAMA Trunk Interface Card	X	X	X

Multiflex Voice/WAN y WIC

Product Number	Description	261x-265x	2600XM	2691
VWIC-1MFT-T1	1-port T1/Fractional T1 Multiflex Trunk with CSU/DSU	X	X	X
VWIC-2MFT-T1	2-port T1/Fractional T1 Multiflex Trunk with CSU/DSU	X	X	X
VWIC-2MFT-T1-DI	2-port T1/Fractional T1 Multiflex Trunk with CSU/DSU and Drop & Insert	X	X	X
VWIC-1MFT-E1	1-port E1/Fractional E1 Multiflex Trunk with DSU	X	X	X
VWIC-2MFT-E1	2-port E1/Fractional E1 Multiflex Trunk with DSU	X	X	X
VWIC-2MFT-E1-DI	2-port E1/Fractional E1 Multiflex Trunk with DSU and Drop & Insert	X	X	X
VWIC-1MFT-G703	1-port G.703 Multiflex Trunk	X	X	X
VWIC-2MFT-G703	2-port G703 Multiflex Trunk	X	X	X
WIC-1DSU-T1	T1/Fractional T1 CSU/DSU	X	X	X
WIC-1DSU-T1-V2	T1/Fractional T1 CSU/DSU (Replaces WIC-1DSU-T1)		X	X
WIC-1DSU-56K	1-port four-wire 56/64 Kbps CSU/DSU	X	X	X
WIC-1T	1-port high speed serial	X	X	X
WIC-2T	2-port high speed serial	X	X	X
WIC-2A/S	2-port async/sync serial	X	X	X
WIC-1B-S/T	1-port ISDN BRI	X	X	X
WIC-1B-U-V2	1-port ISDN BRI with NT1	X	X	X
WIC-1AM	1-port Analog Modem interface card	X	X	X
WIC-2AM	2-port Analog Modem interface card	X	X	X
WIC-1ADSL	1-port ADSL over POTs WAN Interface	X	X	X
WIC-1ADSL-I-DG	1-port ADSL over ISDN WAN Interface		X	X
WIC-1SHDSL	1-port G.SHDSL WAN Interface	X	X	X
VWIC-1MFT-T1	1-port T1/Fractional T1 Multiflex Trunk with CSU/DSU	X	X	X

MÓDULOS DE INTEGRACIÓN AVANZADA (AIM)

Product Number	Description	2612	2600XM	2691
AIM-COMPR2	Data Compression AIM for the Cisco2600 Series	X	X	
AIM-COMPR4	Data Compression AIM for the Cisco2691, 3660 and 3700 Series			X
AIM-VPN/BP	DES/3DES Data VPN Encryption AIM for the Cisco 2600 Series	X	X	
AIM-VPN/BPII	DES/3DES/AES VPN Encryption & Compression Module for 2600XM		X	
AIM-VPN/EP	DES/3DES Data VPN Encryption AIM for the Cisco 2600 Series	X	X	X
AIM-VPN/EP	DES/3DES/AES VPN Encryption & Compression Module for 2691/3725			X
AIM-ATM	High Performance ATM Advanced Integration Module	X	X	X
AIM-VOICE-30	30-Channel T1/E1 Digital Voice Module	X	X	X
AIM-ATM-VOICE-30	ATM SAR and 30 Channel T1/E1 Digital Voice Module	X	X	X

MÓDULOS DE RED (NM)

Product Number	Description	2612	2600XM	2691
NM-4T1-ATM	4-port T1 ATM with IMA NM	X	X	X
NM-4E1-ATM	4-port E1 ATM with IMA NM	X	X	X
NM-8T1-ATM	8-port T1 ATM with IMA NM	X	X	X
NM-8E1-ATM	8-port E1 ATM with IMA NM	X	X	X
NM-1A-OC3MM	Single-port ATM OC-3 Multimode Network Module (up to 2 km)			X
NM-1A-OC3MI	Single port ATM OC-3 Single mode Intermediate Reach Network Module (up to 15 km)			X
NM-1A-OC3ML	Single-port ATM OC-3 Single Mode Long Reach Network Module (up to 45km)			X
NM-1A-T3	1-Port DS3 ATM NM	X	X	X
NM-1A-E3	1-Port E3 ATM NM	X	X	X
NM-16A	16-port High Density Async NM	X	X	X
NM-32A	32-port High Density Async NM	X	X	X
NM-4A/S	4-port Low Speed (128 Kbps max) Async/Sync Serial NM	X	X	X
NM-8A/S	8-port Low Speed (128 Kbps max) Async/Sync Serial NM	X	X	X
NM-16A/S	16-port Async/Sync Serial NM		X	X
NM-4T	4-port Serial Network Module			X
LAN/LAN/WAN Network Modules				
NM-2FE2W	2-10/100 Ethernet 2- WAN Card Slot Network Nodule			X
NM-1FE2W	1-10/100 Ethernet 2- WAN Card Slot Network Module			X
NM-1FE1R2W	1-10/100 Ethernet 14/16 Token-Ring 2-WAN Card Slot network module			X
NM-1FE-FX	1-port Fast Ethernet Network Module, FX Only			X
NM-1FE-FX-V2	1-port Fast Ethernet Network Module, FX Only			X
NM-2W	2-WAN Interface Card Slot Network Module, (WAN I/F cards offered separately)	X	X	X
NM-1E	1-port Ethernet Network Module	X	X	
NM-4E	4-port Ethernet Network Module	X	X	
NM-1ATM-25	1-port ATM 25Mbps Network Module	X	X	
NM-1GE	1-port Gigabit Ethernet Network Module			X
NM-1T3/E3	1-port Clear Channel		X	X
Dial, ISDN, Analog Modems & Chan Serial Network Modules				
NM-1CE1T1-PRI	1-port Channelized E1/T1/ISDN PRI Network Module		X	X
NM-2CE1T1-PRI	2-port Channelized E1/T1/ISDN PRI Network Module		X	X
NM-1CT1	1-port Channelized T1/ISDN PRI Network Module	X	X	X
NM-1CT1-CSU	1-port Channelized T1/ISDN PRI with CSU Network Module	X	X	X
NM-2CT1	2-port Channelized T1/ISDN PRI Network Module	X	X	X
NM-2CT1-CSU	2-port Channelized T1/ISDN PRI with CSU Network Module	X	X	X
NM-1CE1B	1-port Channelized E1/ISDN PRI Balanced Network Module	X	X	X
NM-1CE1U	1-port Channelized E1/ISDN PRI Unbalanced Network Module	X	X	X
NM-2CE1B	2-port Channelized E1/ISDN PRI Balanced Network Module	X	X	X
NM-2CE1U	2-port Channelized E1/ISDN PRI Unbalanced Network Module	X	X	X
NM-4B-S/T	4-port ISDN BRI Network Module (S/T interface)	X	X	X

NM-4B-U	4-port ISDN BRI with NT-1 Network Module (U interface)	X	X	X
NM-8B-S/T	8-port ISDN BRI Network Module (S/T interface)	X	X	X
NM-8B-U	8-port ISDN BRI with NT-1 Network Module (U interface)	X	X	X
NM-8AM	8-analog Modem Network Module	X	X	X
NM-16AM	16-analog Modem Network Module	X	X	X
NM-1HSSI	1-port HSSI Network Module			X
Voice/Fax Network Modules				
NM-HDV-1T1-12	12-channel T1 High Density Voice/Fax Network Module	X	X	X
NM-HDV-1E1-12	12-channel E1 High Density Voice/Fax Network Module	X	X	X
NM-HDV-1T1-24	24-channel T1 High Density Voice/Fax Network Module	X	X	X
NM-HDV-1T1-24E	24-channel T1 Enhanced High Density Voice/Fax Network Module	X	X	X
NM-HDV-1E1-30	30-channel E1 High Density Voice/Fax Network Module	X	X	X
NM-HDV-1E1-30	30-channel Enhanced E1 High Density Voice/Fax Network Module	X	X	X
NM-HDV2	IP Communications High-Density Digital Voice/Fax Network Module		X	X
NM-HDV2-1T1/E1	IP Communications High-Density Digital Voice/Fax Network Module with One Built-in T1/E1 port		X	X
NM-HDV2-2T1/E1	IP Communications High-Density Digital Voice/Fax Network Module with Two Built-in T1/E1 ports		X	X
NM-HDV-2T1-48	48-channel T1 High Density Voice/Fax Network Module	X	X	X
NM-HDV-2E1-60	60-channel E1 High Density Voice/Fax Network Nodule	X	X	X
NM-1V	1-slot Voice/Fax Network Module	X	X	X
NM-2V	2-slot Voice/Fax Network Module	X	X	X
NM-16ESW-PWR	16 Port 10/100 Etherswitch NM with Power card	X	X	X
NM-16ESW	16-Port 10/100 Etherswitch NM	X	X	X
EM-HDA-8FXS	8-Port voice/fax Expansion Module FXS	X	X	X
NM-HDA-4FXS	High Density Analog Voice/Fax Network Module with 4 FXS	X	X	X
EM-HDA-4FXO	4-Port Voice/Fax Expansion Module FXO	X	X	X
NM-HDV-1J1-30	1-port 30-Channel J1 High-Density Voice Network Module	X	X	X
NM-HDV-1J1-30E	1-Port 30-Enhanced Channel J1 High-Density Voice Network	X	X	X
NM-HDV-FARM-C36	Network Module 36- Port DSP Farm Bundle	X	X	X
NM-HDV-FARM-C54	Network Module 54- Port DSP Farm Bundle	X	X	X
NM-HDV-FARM-C90	Network Module 90- Port DSP Farm Bundle	X	X	X
NM-HD-1V	One-slot IP Communications Voice/Fax Network Module		X	X
NM-HD-2V	2-slot IP Communications Voice/Fax Network Module		X	X
NM-HD-2VE	2-slot IP Communications Enhanced Voice/Fax Network Module		X	X
Alarm Interface Controller (AIC) Network Modules				
NM-AIC-64	Alarm monitoring and Control NM; 64 Contact Points and 16-control points	X	X	X
Intrusion Detection System Network Modules				
NM-CIDS-K9	Cisco IDS Network Module, 20-GB IDE Hard Disk		X	X
Content Engine Network Modules				
NM-CE-BP-20G-K9	Content Engine Network Module, Basic Performance, 20-GB IDE Hard Disk	X	X	X
NM-CE-BP-40G-K9	Content Engine Network Module, Basic Performance, 40-GB IDE Hard Disk	X	X	X
NM-CE-BP-SCSI-K9	2-port E&M Voice/Fax Interface Card for Voice/Fax Network Module	X	X	X

ANEXO E. CONTENIDO DEL CD ROM ADJUNTO

- Monografía Documento
- Monografía Investigación
  - Ancho de Banda
  - ATM
  - Cisco: IOS - Router
  - Otros temas
- Aplicaciones Útiles

ANEXO F. AGRADECIMIENTO ESPECIAL A ORGANIZACIONES

Por su dedicación en el desarrollo de aplicaciones útiles a toda la comunidad.

Opera

www.opera.com

OpenOffice.org

www.openoffice.org

Por permitir que la comunidad pueda ver de primera mano los trabajos que desarrollan en función de la estandarización de sus respectivas tecnologías

Cisco Documentation

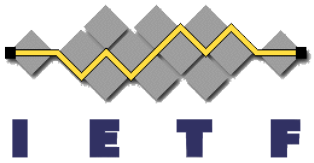
www.cisco.com/univercd/

ATM Forum

www.atmforum.com

Internet Engineering Task Force (IETF)

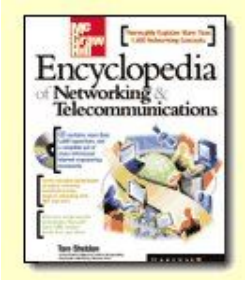
www.ietf.org



Por realizar un extraordinario trabajo en recopilar información acerca de las tecnologías de telecomunicaciones.

Encyclopedia of Networking and Telecommunicatons

www.linktionary.com



AUTORIZACIÓN

Cartagena de Indias, D.T. y C., 23 de junio de 2004

Nosotros GUSTAVO ADOLFO AGUDELO FRÍAS y FERNANDO DE ORO BARRIOS, autorizamos a la Universidad Tecnológica de Bolívar para hacer uso de nuestra monografía titulada “TÉCNICAS PARA LA GESTIÓN DEL ANCHO DE BANDA EN LA WAN CON SOPORTE EN ROUTERS CISCO 2600” y pueda ser publicada en el catálogo en línea de la Biblioteca Luis Enrique Borja Barón.

Atentamente,

GUSTAVO ADOLFO AGUDELO FRÍAS	FERNANDO DE ORO BARRIOS
C.C. ##.###.### de Cartagena	C.C. ##.###.### de Cartagena