MPLS/VPLS

SERVICIO DE LAN PRIVADA VIRTUAL SOBRE MPLS

VICTOR HUGO OSPINA

JUAN ARMANDO ZAJAR

UNIVERSIDAD TECNOLÓGICA DE BOLIVAR

FACULTAD DE INGENIERIAS

DIRECCIÓN DEL PROGRAMA DE INGENIERIA DE SISTEMAS

CARTAGENA DE INDIAS D. T. Y C

2005

MPLS/VPLS

SERVICIO DE LAN PRIVADA VIRTUAL SOBRE MPLS

VICTOR HUGO OSPINA

JUAN ARMANDO ZAJAR

Monografía presentada como requisito de aprobación del Minor en Comunicaciones y Redes

Director

ISAAC ZUÑIGA SILGADO

Ingeniero de Sistemas

UNIVERSIDAD TECNOLÓGICA DE BOLIVAR

FACULTAD DE INGENIERIAS

DIRECCIÓN DEL PROGRAMA DE INGENIERIA DE SISTEMAS

CARTAGENA DE INDIAS D. T. Y C

2005

Nota de Aceptación

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Cartagena, Agosto 11 de 2005

Cartagena, Agosto 11 de 2005

Señores

COMITÉ DE REVISIÓN DE MONOGRAFÍA

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

La Ciudad

Apreciados señores:

Por medio de la presente nos permitimos informarles que la monografía titulada "**MPLS/VPLS: SERVICIO DE LAN PRIVADA VIRTUAL SOBRE MPLS"** ha sido desarrollada de acuerdo a los objetivos establecidos.

Como autores del proyecto consideramos que el trabajo es satisfactorio y amerita ser presentado para su evaluación.

Atentamente,

_____	_____
VICTOR HUGO OSPINA	**JUAN ARMANDO ZAJAR**
C.C 18.469.057	C.C 73.180.570

Cartagena, Agosto 11 de 2005

Señores

COMITÉ DE REVISIÓN DE MONOGRAFÍA

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

La Ciudad

Apreciados señores:

Por medio de la presente me permito informarles que la monografía titulada "**MPLS/VPLS: SERVICIO DE LAN PRIVADA VIRTUAL SOBRE MPLS"** ha sido desarrollada de acuerdo a los objetivos establecidos.

Como director considero que el trabajo es satisfactorio y amerita ser presentado para su evaluación.

Atentamente,

_____

ISAAC ZUÑIGA SILGADO
Ingeniero de Sistemas
Magíster en Redes (C)

AUTORIZACIÓN

Cartagena de Indias D. T. y C

Agosto 11 de 2005

Yo VICTOR HUGO OSPINA URIBE, identificado con la cédula de ciudadanía número 18.469.057 del Municipio de Quimbaya-Quindío. Autorizo a la Universidad Tecnológica de Bolívar a hacer uso de mi trabajo de grado y publicarlo en el catálogo ON LINE de la Biblioteca.

_____

VICTOR HUGO OSPINA URIBE

AUTORIZACIÓN

Cartagena de Indias D. T. y C

Agosto 11 de 2005

Yo JUAN ARMANDO ZAJAR, identificado con la cédula de ciudadanía número 73'180.570 de la ciudad de Cartagena. Autorizo a la Universidad Tecnológica de Bolívar a hacer uso de mi trabajo de grado y publicarlo en el catálogo ON LINE de la Biblioteca.

_____

JUAN ARMANDO ZAJAR

ARTICULO 105

La Universidad Tecnológica de Bolívar, se reserva el derecho de propiedad intelectual de todos los trabajos de grado aprobados, y no pueden ser explotados comercialmente sin autorización.

AGRADECIMIENTOS

Los autores expresan sus agradecimientos:

Ante todo a Dios por habernos dado las capacidades suficientes para desarrollar la investigación.

A nuestros padres por el apoyo incondicional que nos han ofrecido para la consecución de nuestros estudios.

A la compañía Riverstone por haberse preocupado por nuestra investigación y habernos facilitado artículos relacionados con el tema.

A nuestro director, **ING. ISAAC ZUÑIGA SILGADO** por su colaboración y guía en el desarrollo del trabajo.

CONTENIDO

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

ACRONIMOS

AAL	ATM Adaptation Layer
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BUS	Broadcast and Unknown Server
CAC	Connection Admission Control
CBR	Constraint Based Routing
CE	Customer Edge router
CIDR	Classless Inter-Domain Routing
CoS	Class of Service
CPCS	Common Part Convergence Sublayer
CR-LDP	Constraint-Based Routing Label Distribution Protocol
DiffServ	Differentiated Services
EBW	Effective Bandwith
FEC	Forwarding Equivalence Class
GMPLS	Generalized MPLS
IETF	Internet Engineering Task Force
IGMP	Internet Group Multicast Protocol.
IGP	Interior Gateway Protocol
INNI	Internal node-to-node interface
IntServ	Integrated Services
IP	Internet Protocol
IS-IS	Intermediate System - Intermediate System routing protocol
ISP	Internet Service Provider
ITU – T	International Telecommunication Union Telecomm Standardization
LANE	Lan Emulation
LDP	Label Distribution Protocol.
LEC	Lan Emulation Client
LEC	Lan Emulation Configuration Client
LES	Lan Emulation Server

LLC	Logical Link Control
LSP	Label Switch Path.
LSR	Label Switched Router
MPLS	Multiprotocol Label Switching
OAM	Operation, Administration and Maintenance.
OIF	Optical Internetworking Forum
OSPF	Open Shortest Path First routing protocol
OTN	Optical Transport Network
OXC	Optical Cross-Connect
P	Provider (core) router
PBNM	Policy Based Network Management
PDU	Protocol Data Unit
PE	Provider Edge router (Label Edge Router o LER).
PIM	Protocol Independent Multicast.
P	Provider switch (Label Switch Router o LSR).
PSTN	Public Switched Telephone Network
PWE	Pseudo Wired Ethernet
PWP	seudo-wire.
QoS	Quality of Service
RSVP	Resource Reservation Protocol
SAP	Service Access Point
SDH	Synchronous Digital Hierarchy
SNAP	SubNetwork Attachment Point
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical NETwork
TE	Traffic Engineering
TI	Tecnología de la Información
TMN	Telecommunications Management Network
UNI	User to Network Interface
VC	Virtual Circuit
VLAN	Virtual Lan
VoIP	Voice over IP
VPLS	Virtual Private Lan Services
VPN	Virtual Private Network

VSI	Virtual Switching Instance
WAN	Wide Area Network
WDM	Wavelenght División Multiplexing

RESUMEN

En la actualidad MPLS se ha convertido en una de las soluciones más apetecidas para la implementación del transporte en Backbones metropolitanos, las ventajas de una red Multiservicio sobre una red IP son innumerables entre ellas están la implementación de soluciones Ethernet punto a punto en las cuales dos equipos remotos pueden compartir el mismo dominio de broadcast; en estos momentos se esta trabajando en la implementación de VPNs de nivel 2 que permitan solucionar el problema de la conversión de direcciones MAC a IP.

Dentro de los antecedentes de las investigaciones sobre la emulación de redes LAN en Backbones, encontramos ATM LANE que emulaba una LAN sobre una WAN ATM, el servicio ATM LANE tenía 4 componentes básicos. Un LEC (Lan Emulation Client), un LECS (Lan Emulation Configuration Server), un LES (Lan Emulation Server) y un BUS (Broadcast Unknow Server), estos componentes interactúan Emulando una LAN en la cual los LEC comparten un mismo dominio de Broadcast; otro antecedente importante tiene que ver con AAL5 y con su mecanismo "LLC Encapsulation" que multiplexa varios protocolos sobre un mismo circuito virtual.

Cuando se habla de VPLS es de vital importancia hacer un repaso por los conceptos más importantes de MPLS, explicar como opera el Backbone MPLS con todos sus componentes entre ellos los LSR (Label Switching Router), como se realiza el intercambio de etiquetas y como este intercambio de etiquetas optimiza el envío de paquetes en la red.

Finalmente entramos a discutir los conceptos más importantes acerca de VPLS, que se define como una implementación de VPN de nivel 2 caracterizado por el soporte de difusión de capa 2, se explican los conceptos acerca del trabajo en VPLS, el funcionamiento de las etiquetas PWe que solo tienen validez en los PE de entrada y salida. Por ultimo se realiza un breve resumen de los nuevos trabajos como son H-VPLS (VPLS jerárquico) y H-VPLS Inter.-operadores, Inter.-dominios (VPLS entre dominios).

INTRODUCCIÓN

En la actualidad las investigaciones en el campo de las telecomunicaciones se han convertido en una prioridad para las empresas desarrolladoras de hardware y de software; con la demanda actual de ancho de banda que requieren algunas aplicaciones como el video, la voz sobre IP y algunas aplicaciones corporativas, es necesario crear mecanismos en las redes de los proveedores de servicios que optimicen el ancho de banda, que puedan operar sobre las infraestructuras ya existentes y además que operen de forma transparente con los protocolos subyacentes.

La presente monografía tiene por objeto mostrar la evolución de las telecomunicaciones a nivel de redes de operador; mostrar las tecnologías que se han venido utilizando a lo largo de los años hasta llegar ha MPLS/VPLS; dentro de estos antecedentes se encuentra ATM/LANE, AAL5 que emulaban redes LAN sobre infraestructuras ATM. También se muestra la evolución de la tecnología de conmutación, repasando algunos conceptos básicos sobre conmutación y haciendo énfasis en lo que respecta a STP (Spanning Tree Protocol) y VLANS que son conceptos de mucha importancia para poder comprender el funcionamiento de la tecnología VPLS.

Luego de haber repasado los conceptos de conmutación se hace una introducción a MPLS que es la tecnología utilizada por VPLS, la idea fundamental de la teoría expuesta de MPLS es explicar su funcionamiento el intercambio de etiquetas en los LSR, el proceso de selección de los LSP y el funcionamiento de los protocolos RSVP y LPD.

A continuación se expone el funcionamiento de MPLS/VPLS haciendo una introducción para explicar los conceptos y como se comporta un Backbone metropolitano en el cual opera VPLS; el funcionamiento de VPLS es un aspecto fundamental de la monografía, se trató de hacer una explicación sintetizada y clara de cómo opera VPLS y como hace que el backbone metropolitano se

perciba como un gran Switch único, los temas adicionales como H-VPLS y VPLS Inter-dominios / Inter-operadores se trataron someramente pero siempre tratando de enumerar las ventajas que este tipo de tecnología trae para los proveedores del servicio de internet.

Finalmente se presenta un ejemplo real de una topología sencilla sobre la cuál se implementa VPLS, este ejemplo le permite al lector tener una idea más clara y real de la operación de VPLS, sus ventajas y limitaciones.

1. PLANTEAMIENTO DEL PROBLEMA.

En la actualidad los operadores de Internet están evolucionando hacia una infraestructura de red común basada en paquetes, sobre la cuál se pueda transportar voz, datos y video; esta infraestructura de red exige que los operadores del servicio deban buscar nuevas tecnologías para ofrecerles a sus usuarios Calidad de Servicio, sin necesidad de invertir grandes cantidades de dinero en nuevas infraestructuras.

Como resultado de la necesidad de ofrecer una infraestructura de redes convergente, las empresas fabricantes de dispositivos de redes están trabajando en el desarrollo de nuevas tecnologías para que los operadores puedan ofrecer nuevos servicios económicos, eficientes y confiables; Inicialmente estos nuevos servicios se basaban en Ethernet, como una UNI de servicio para usuarios finales y también como una tecnología de conmutación / transporte.

En un principio los switches Ethernet ordinarios se usaban para este tipo de transporte. Los requisitos eran soportar toda la gama de VLANs 802.1Q (4096) y tener la capacidad para manejar una gran cantidad de direcciones MAC. Rápidamente surgieron requisitos nuevos para escalar y operar de manera rentable las dorsales Ethernet del proveedor del servicio (SP):

- Capacidad para soportar la conversión VLANs para manejar clientes con VLANs traslapadas.

- Capacidad para transportar de manera transparente las BPDUs de Árbol en expansión (STP) del cliente.

- Capacidad para manejar una gama completa de VLANs por cliente, independientemente de las VLANs del proveedor de servicio, conocidas como QinQ.

El grupo de trabajo IEEE 802.1ad estandarizó recientemente estas extensiones. Se agregaron mejoras al protocolo de Árbol en expansión (STP); por ejemplo, el Árbol en expansión rápida (802.1w) para lograr una convergencia más rápida y VLANs múltiples por instancia de Árbol en expansión (802.1s) para la ingeniería de tráfico básica.

Rápidamente fue necesario proveer una propuesta más escalable para operar dichas redes. Esto implicaba que los conmutadores (switches) usados para el transporte tenían que ser de clase operador (carrier-class). En otras palabras, tenían que proporcionar la misma confiabilidad, escalabilidad y capacidades de seguridad que las que ofrecían los switches tradicionales TDM o ATM. MPLS tiene la mayoría de los atributos requeridos para enfrentar dichos retos, ya que cuenta con sólidas capacidades de "tunelización", ingeniería de tráfico, calidad de servicio (QoS) y protección rápida.

Una de los principales servicios derivados de la tecnología MPLS es VPLS, este servicio permite la conectividad multipunto y habilita los servicios LAN a LAN, permitiéndole al operador optimizar los servicios de interconexión de redes corporativas ubicadas sobre un mismo backbone metropolitano, VPLS es la solución para que los operadores del servicio ofrezcan un mejor rendimiento y Calidad de servicio a sus suscriptores principalmente a las corporaciones que requieren de servicios de transporte nuevos, más económicos, rápidos y flexibles que las líneas arrendadas tradicionales.

2. OBJETIVOS

2.1 OBJETIVO GENERAL.

Conceptuar todas las características de VPLS, haciendo énfasis en los aspectos técnicos, productos disponibles y ventajas para los operadores del servicio de Internet.

2.2 OBJETIVOS ESPECIFICOS.

- Identificar y explicar la evolución de las tecnologías de transporte a nivel de redes metropolitanas hasta llegar a VPLS.

- Explicar los conceptos más relevantes de la tecnología MPLS.

- Exponer las ventajas y desventajas de VPLS.

- Profundizar en los aspectos técnicos funcionales y arquitectónicos de la tecnología VPLS.

- Analizar y explicar los conceptos de H-VPLS y H-VPLS Interdominios / Interoperadores.

- Implementar un prototipo de prueba de VPLS sobre routers CISCO.

3. JUSTIFICACIÓN

En los últimos años la industria de las redes de comunicaciones y las organizaciones encargadas del desarrollo tecnológico, han dado grandes pasos en el desarrollo de nuevas tecnologías que beneficien a los proveedores de servicios de internet y a los usuarios de la red; el estudio de estas tecnologías es de suma importancia para las personas involucradas con el mundo del internetworking.

VPLS es una de las tecnologías más importantes derivadas de MPLS, desde la introducción de la tecnología MPLS los operadores del servicio han experimentado múltiples beneficios que hacen importante el estudio de estas tecnologías que ya se encuentran en el mercado y que están siendo implementadas en estos momentos.

Entre los beneficios más importantes que trae consigo la nueva tecnología MPLS/VPLS se encuentran:

- Ingeniería de tráfico.
- Calidad de Servicio.
- Reestablecimiento rápido de los enlaces.
- El reemplazo de las antiguas líneas arrendadas.
- Servicios corporativos LAN a LAN.
- Migración sin problemas de la base de clientes.
- Escalabilidad.
- Multicast mejorado.
- Alta disponibilidad de las redes.
- Localización de fallas de extremo a extremo.
- Prestación rápida de servicios.
- Servicios en zonas geográficas amplias con QoS entre operadores.
- Facilidad de aprovisionamiento, localización de fallas.
- Servicios múltiples desde una plataforma.

Todos estos beneficios listados anteriormente convierten a MPLS/VPLS en un tema importante para el desarrollo de investigaciones universitarias,

puesto que a corto plazo se convertirá en la tecnología estándar para transporte de datos en backbones metropolitanos.

Por otra parte es importante realizar esta investigación para medir el impacto de esta tecnología en aspectos tan importantes como la creación de LAN privadas virtuales en topologías jerárquicas e interdominios / interoperadores.

Incrementar el material de consulta en nuevas tecnologías es importante desde todo punto de vista, puesto que esto sienta un punto de inicio para el desarrollo de proyectos de investigación más extensos, que conlleven a la consolidación y acreditación de los programas que se desarrollan dentro de la universidad.

4. ANTECEDENTES DE VPLS.

Desde su introducción MPLS ha tenido un gran suceso como el protocolo de transporte elegido por diferentes proveedores en sus núcleos (backbones).

Las ventajas de una red Multiservicio sobre una red IP pura son innumerables, para un proveedor la primera que surge tiene que ver con el desarrollo de Redes Privadas de nivel 3. Esta tecnología permite pasar del viejo modelo de apiñamiento de protocolos (para las VPN de nivel 2) a un modelo compartido. Así únicamente existe conmutación de etiquetas con un plano de control fuerte, permitiendo una gestión integrada, con beneficios para la operación y siendo un modelo fácilmente escalable.

Pero si un proveedor planifica construir un núcleo de red integrado, deberá transportar en él todos sus servicios, en especial los viejos servicios legacy donde los protocolos a utilizar hacia el cliente son Frame Relay, ATM o Ethernet. El transporte en cada uno de éstos sobre un núcleo MPLS trae dificultades muy interesantes, en especial en lo referido al transporte de protocolos orientados a conexión sobre IP, las adaptaciones de los planos de control, entre otros.

El primer problema donde se ha encontrado una solución es el transporte de tramas Ethernet sobre MPLS para conexiones punto a punto. De esta forma se logra que dos equipos en puntos diferentes de una red MPLS (compuestas por LSRs de capa 3) logren compartir un dominio de broadcast.

Este tipo de soluciones son interesantes en conexiones de grandes anchos de banda, en general a través de fibras ópticas, donde se busca conectividad entre un Centro de Datos principal y otro secundario. Un problema aún planteado es la posibilidad de construir una VPN de nivel 2 a través del transporte de Ethernet sobre MPLS, aquí aparece el inconveniente de tener que realizar una conversión entre dirección MAC y dirección IP del Edge-LSR (PE) correspondiente.

Tradicionalmente existen soluciones para el transporte de tramas Ethernet sobre un núcleo ATM. Básicamente se destacan dos soluciones, la primera basada en el estándar Lan Emulation del ATM Forum y la segunda basada en el transporte sobre AAL5, RFC1483 (sustituida por RFC 2684[1]).

4.1 ATM LANE.

Definido por el ATM Forum en el año 1995 para simular un ambiente LAN sobre una nube WAN ATM. De esta forma toma los beneficios a nivel de QoS y control de ancho de banda de ATM, manteniendo hacia el usuario las características de simpleza de su infraestructura LAN ya instalada.

Si relevamos las características de un servicio LAN encontramos los siguientes aspectos: alta velocidad, posibilidad de realizar difusiones, servicio no orientado a conexión y operación automática (plug and play). ATM cumple claramente con la premisa respecto a la velocidad, LANE resuelve el resto de las características planteadas.

Componentes y Conexiones para LANE:

En la figura 1 se muestran un esquema general LANE donde se aprecian las conexiones virtuales que interconectan cuatro componentes lógicos:

- LAN Emulation Client (LEC)
- LAN Emulation Configuration Server (LECS)
- LAN Emulation Server (LES)
- Broadcast and Unknown Server (BUS)

[1] Multiprotocol Encapsulation over ATM Adaptation Layer 5", D. Grossman, J. Heinanen, RFC 2684

Un LEC corre en cada elemento de red ATM que pertenece al dominio de difusión que se intenta simular sobre ATM. Puede ser sobre un servidor particular con interfaz ATM (por ejemplo interfaces de 25Mbps sobre cobre), un enrutador o un puente. Cada LEC tendrá asociada una dirección ATM E.164 única. Cada LEC se asocia a un ambiente LANE conectándose a un LECS a través de un ATM SVC (claramente va a necesitar configurarle la dirección ATM de el LECS correspondiente o descubrirla a través del protocolo ILMI).

Dentro de cada dominio administrativo existirá un único LECS, que puede atender varias LANes. Cuando un cliente se conecta con él éste lo redirige hacia el LES que controla el segmento a donde el cliente pertenece, terminando su participación en la asociación del cliente.

La función del LES es implementar y mantener el registro de direcciones y realizar la conversión de direcciones MAC a direcciones ATM. Cuando un LEC se registra con su LES (asignado por el LECS), envía su dirección MAC y su dirección ATM. El LES asignará a cada LEC la dirección del BUS correspondiente al dominio que pertenece.

El servidor BUS se utiliza para la difusión de tramas destinadas a usuarios desconocidos y para tráfico broadcast y multicast entre los clientes de una Emulated LAN (ELAN). Cada ELAN puede tener más de un BUS (por razones de uso de recursos de red), pero cada LEC trasmite únicamente a uno de ellos.

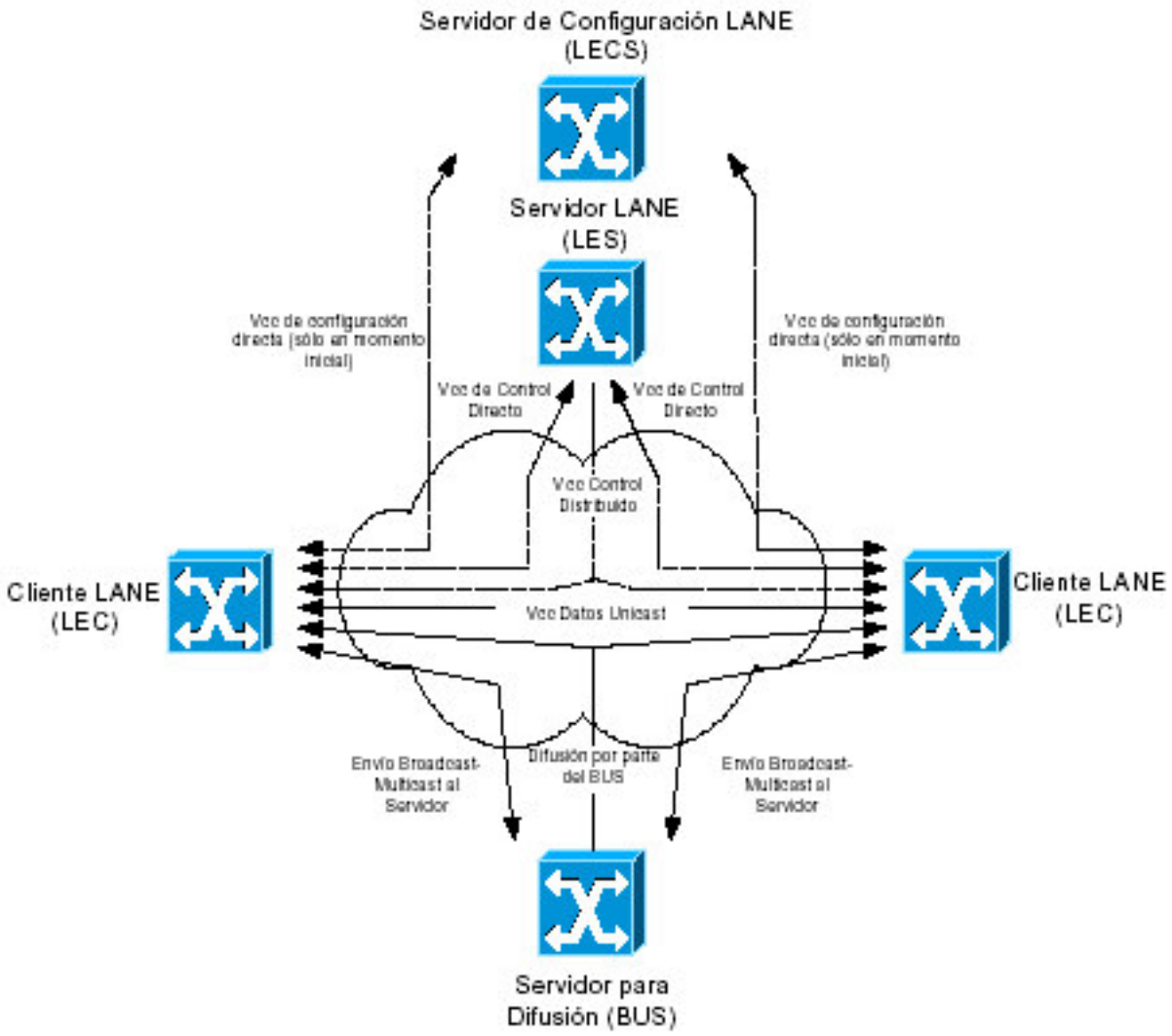

Fig. 1

Luego de la etapa de asociación, cuando un LEC requiere comunicarse en forma unicast con un equipo a través de la red ATM, envía un pedido de resolución a su LES indicando la MAC de destino (LE-ARP). El servidor contestará con la dirección ATM de destino (si el usuario ya se ha registrado) o enviará el pedido a otro LEC que pueda responderlo. Una vez recibida la dirección ATM del destinatario el cliente establece una conexión de datos con él y a través de estos SVC se envían las tramas de información (utilizando RFC1483[2]).

[2] Multiprotocol Encapsulation over ATM Adaptation Layer 5", Juha Heinanen, RFC 1483.

Durante la espera de la respuesta del LES es posible enviar el primer paquete en forma de difusión (a través del BUS) para evitar su almacenamiento en el cliente o la pérdida del mismo.

El proceso de difusión consiste en el envío del paquete hacia el BUS, luego éste lo envía al resto de los clientes a través de una conexión punto-multipunto. Dado que cada cliente vuelve a recibir las tramas que él ha trasmitido, a la trama LANE se agrega una identificación del LEC originador.

Si un cliente no recibe respuesta desde el LES a su pedido LE-ARP, continúa enviando la información a través del BUS.

4.2 ENCAPSULAMIENTO MULTIPROTOCOLO SOBRE AAL5.

IETF RFC 1483 (actualizado por RFC 2684) define la forma de transporte de diferentes protocolos sobre la capa de adaptación ATM AAL5 (ITU-T I.363.5 [3]). Este documento estandariza el transporte a través del enrutamiento de los paquetes de capa superior (como pueden ser paquetes IP) como así también el bridging de tramas de capa 2 a través de circuitos ATM.

Se definen dos escenarios posibles para el ruteo o el bridging, por un lado la opción “LLCencapsulation” consiste en la multiplexación sobre un mismo VC (Circuito Virtual) de diferentes protocolos, en cambio la opción “VC-multiplexing” consiste en separa en diferentes VC los diferentes protocolos. La elección de una u otra opción va a depender de la solución a implementar aunque en general la solución LLC requieren menos VCs y por ende menor mantenimiento mientras que la solución VC trae menos encabezados.

---

[3] ITU-T Recommendation I.363.5, "B-ISDN ATM Adaptation Layer (AAL) Type 5 Specification", August 1996.

El método de conexión es posible negociarlo si es que se deciden utilizar SVCs.
Aquí solo detallamos el encapsulamiento LCC como ejemplo. Este tipo de encapsulamiento es necesario cuando diferentes protocolos comparten un mismo VC ATM, de forma que el receptor pueda interpretar correctamente el contenido del AAL5 CPCS-PDU. Por lo tanto la intención es identificar correctamente el protocolo, ya sea enrutado o bridgeado, dentro de éste PDU.

La solución consiste en transportar dentro de este campo el encabezado 802.2 LLC, este encabezado está formado por 3 bytes:

DSAP	SSAP	Ctrl

fig. 2

En general para tanto el transporte de paquetes IPs o tramas Ethernet el valor del encabezado 802.2 LLC será siempre AA-AA-03, indicando la presencia de un encabezado 802.1a SNAP para ubicar al protocolo de capa superior dentro del PDU. Otros valores del encabezado LLC identifican otros protocolos enrutados de la ISO (se utiliza la identificación ISO-NLPID).
Por ejemplo para poder transportar paquetes IPs de forma ruteada sobre un VC se tomarían los siguientes valores dentro del PDU AAL5:

	LLC - DSAP	*LLC – SSAP*	*LLC -Ctrl*	*SNAP – OUI*	*SNAP - PID*
Valor (Hex.)	AA	AA	03	00-00-00	08-00

fig. 3

El valor LLC AA-AA-03 identifica que sigue un campo SNAP y el valor PID 08-00 identifica a IP como protocolo de capa superior.

Para el transporte de tramas en forma bridgeada es necesario agregar dos informaciones, el tipo de medio desde donde se originó la trama (sea Ethernet, Tocken Ring, etc.) y si se incluye o no el campo FCS original (para la

corrección de errores en la trama) o se pide el recalculo en el destino, ambas informaciones se encuentran dentro del valor del SNAP-PID a tomar.
En el ejemplo se muestra el transporte de Ethernet 802.3:

	LLC	*SNAP-OUI*	*SNAP-PID*	*PAD*	*Trama MAC*	*LAN FCS*
Valor (Hex.)	AA-AA-03	00-80-C2	00-01 o 00-07	00-00	----------	Sólo si PID= 00-01

fig. 4

La necesidad de un PAD viene dado debido a la necesidad del protocolo 802.3 de tener un tamaño mínimo de trama, el pading es obligatorio cuando se preserva el FCS de la trama original.
Tomemos ahora el ejemplo de una red bridgeada con conexiones AAL5 como se indica en la figura 5.

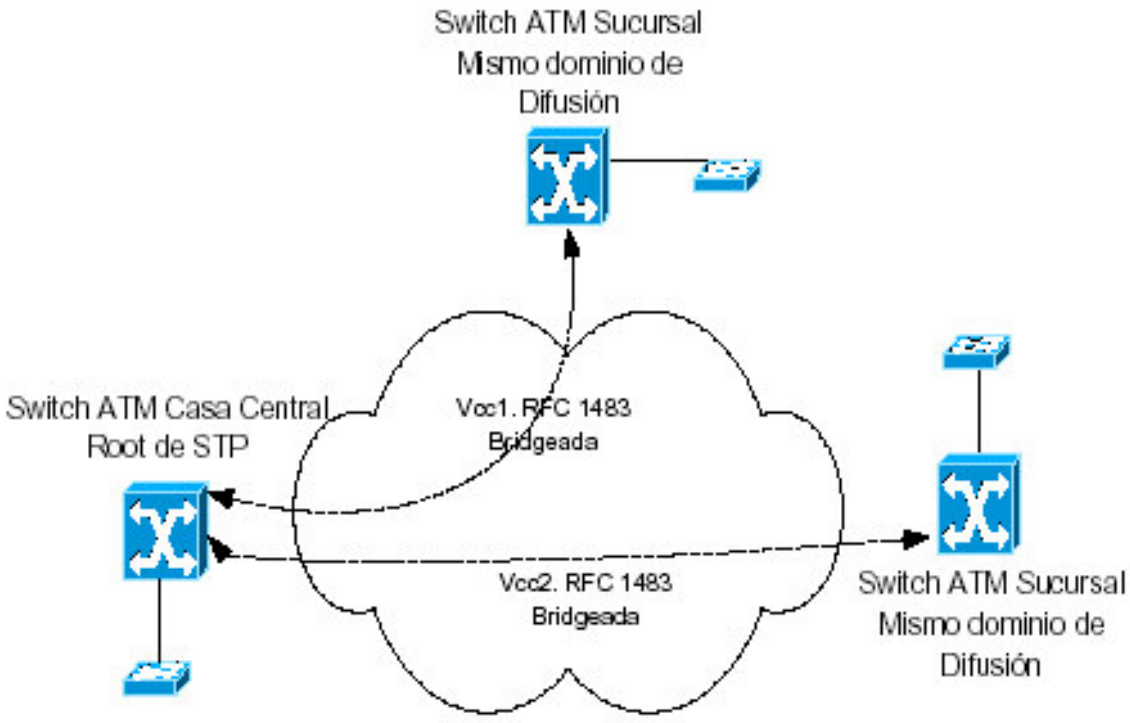

Fig. 5

Luego de tener levantados los diferentes VCs ATM con conexiones AAL5, cada switch ATM es capaz de realizar inundación, transporte y filtrado de tramas entre éstos. Para realizar una inundación, se envía a todos los VCs posibles, ya

sean conexiones punto a punto o conexiones punto-multipunto. Para el transporte de tramas unicast, el switch debe tener una relación entre direcciones MAC y VCs conectados. El llenado de esta tabla se realiza de forma similar a un puente transparente, es decir tomando el campo MAC origen de cada trama que se recibe.

4.3 EVOLUCIÒN DE LA CONMUTACIÒN DE PAQUETES.

A finales de la década de 1990, los operadores competitivos comenzaron a ofrecer servicios de transporte nuevos, más baratos, rápidos y flexibles que las líneas arrendadas tradicionales o los servicios de acceso Frame Relay.
Estos nuevos servicios se basaban en Ethernet, como una UNI de servicio para usuarios finales y pero también como una tecnología de conmutación / transporte.
En un principio, los conmutadores (switches) Ethernet ordinarios se usaban para este tipo de transporte. Los requisitos eran soportar toda la gama de VLANs 802.1Q (4096) y tener la capacidad para manejar una gran cantidad de direcciones MAC. Rápidamente surgieron requisitos nuevos para escalar y operar de manera rentable las dorsales Ethernet del proveedor del servicio (SP):

• Capacidad para soportar la conversión VLANs para manejar clientes con VLANs traslapadas.
• Capacidad para transportar de manera transparente las BPDUs de Árbol en expansión (STP) del cliente.
• Capacidad para manejar una gama completa de VLANs por cliente, independientemente de las VLANs del proveedor de servicio, conocidas como QinQ.

El grupo de trabajo IEEE 802.1ad estandarizó recientemente estas extensiones. Se agregaron mejoras al protocolo de Árbol en expansión (STP); por ejemplo, el Árbol en expansión rápida (802.1w) para lograr una convergencia más rápida y VLANs múltiples por instancia de Árbol en expansión (802.1s) para la ingeniería de tráfico básica.

A continuación se explicarán los conceptos básicos que giran alrededor de la evolución de la tecnología de conmutación de paquetes.

4.3.1 STP (Spanning Tree Protocol).

Las topologías de red redundantes están diseñadas para garantizar que las redes continúen funcionando en presencia de puntos únicos de falla. El trabajo de los usuarios sufre menos interrupciones dado que la red continúa funcionando. Cualquier interrupción provocada por una falla debe ser lo más breve posible.

La confiabilidad aumenta gracias a la redundancia. Una red basada en switches presentará enlaces redundantes entre aquellos switches para superar la falla de un solo enlace. Estas conexiones introducen loops físicos en la red.

Estos loops de puenteo se crean de modo que si un enlace falla, otro enlace puede hacerse cargo de la función de enviar tráfico.

Cuando un switch desconoce el destino del tráfico, inunda el tráfico desde todos los puertos salvo el puerto que recibió el tráfico. Las tramas de broadcast y multicast también se envían por inundación desde todos los puertos, salvo el puerto que recibió el tráfico. Este tráfico puede quedar atrapado en un loop.

En el encabezado de Capa 2, no hay ningún valor de Tiempo de existencia (TTL). Si una trama se envía a una topología con loops de switches de Capa 2, puede circular por el loop indefinidamente. Esto desperdicia ancho de banda e inutiliza la red.

En la Capa 3, el TTL decrece y el paquete se descarta cuando el TTL llega a 0. Esto genera un dilema. Una topología física que contiene loops de conmutación o puenteo es necesaria con fines de confiabilidad, sin embargo, una red conmutada no puede tener loops.

La solución consiste en permitir loops físicos, pero creando una topología lógica sin loops, la topología lógica sin loops se denomina árbol. La topología

resultante es una topología lógica en estrella o en estrella extendida. Esta topología es el spanning tree (árbol de extensión) de la red. Se considera como un spanning tree dado que todos los dispositivos de la red se pueden alcanzar o abarcar.

El algoritmo que se utiliza para crear esta topología lógica sin loops es el algoritmo spanning-tree. Este algoritmo puede tardar un tiempo bastante prolongado para converger. Se desarrolló un nuevo algoritmo denominado algoritmo rapid spanning-tree para reducir el tiempo que tarda una red en calcular una topología lógica sin loops.

4.3.1.1 Protocolo Spanning-Tree

Los puentes y switches Ethernet pueden implementar el protocolo Spanning-Tree IEEE 802.1d y usar el algoritmo spanning-tree para desarrollar una red de ruta más corta sin loops.

La ruta más corta se basa en costos de enlace acumulativos. Los costos de enlace se basan en la velocidad del enlace.

El Protocolo Spanning Tree establece un nodo raíz denominado puente raíz. El Protocolo Spanning-Tree desarrolla una topología que tiene una ruta para llegar a todos los nodos de la red. El árbol se origina desde el puente raíz Los enlaces redundantes que no forma parte del árbol de primero la ruta más corta se bloquean.

Dado que determinadas rutas están bloqueadas, es posible desarrollar una topología sin loops. Las tramas de datos que se reciben en enlaces que están bloqueados se descartan.

El Protocolo Spanning Tree requiere que los dispositivos de red intercambien mensajes para detectar los loops de puenteo. Los enlaces que generan loops se colocan en estado de bloqueo.

Los switches envían mensajes denominados unidades de datos del protocolo

puente (BPDU) para permitir la creación de una topología lógica sin loops. Las BPDU se siguen recibiendo en los puertos que están bloqueados. Esto garantiza que si una ruta o un dispositivo activo falla, se puede calcular un nuevo spanning-tree.

Las BPDU contienen información que permite que los switches ejecuten acciones específicas:

- Seleccionar un solo switch que actúe como la raíz del spanning-tree.
- Calcular la ruta más corta desde sí mismo hacia el switch raíz.
- Designar uno de los switches como el switch más cercano a la raíz, para cada segmento LAN. Este switch se denomina switch designado. El switch designado administra todas las comunicaciones desde la LAN hacia el puente raíz.
- Elegir uno de sus puertos como su puerto raíz, para cada switch que no es un switch raíz. Esta es la interfaz que brinda la mejor ruta hacia el switch raíz.
- Seleccionar puertos que forman parte del spanning-tree. Estos puertos se denominan puertos designados. Los puertos no designados se bloquean.

4.3.1.2 Operación de spanning-tree

Una vez que la red se ha estabilizado, se ha producido la convergencia y hay un spanning-tree por red.

Como resultado, existen los siguientes elementos para cada red conmutada:

- Un puente raíz por red
- Un puerto raíz por puente que no sea raíz
- Un puerto designado por segmento
- Puertos no designados o que no se utilizan

Los puertos raíz y los puertos designados se usan para enviar (F) tráfico de datos.

Los puertos no designados descartan el tráfico de datos. Estos puertos se denominan puertos de bloqueo (B) o de descarte.

4.3.1.3 Selección del puente raíz

La primera decisión que toman todos los switches de la red es identificar el puente raíz. La posición del puente raíz en una red afecta el flujo de tráfico.

Cuando el switch se enciende, se usa el algoritmo spanning tree para identificar el puente raíz. Las BPDU son enviadas con el ID de puente (BID). El BID se compone de una prioridad de puente que asume un valor por defecto de 32768 y la dirección MAC del switch.

Por defecto, las BPDUs se envían cada dos segundos.

Cuando el switch se enciende por primera vez, supone que es el switch raíz y envía las BPDU que contienen la dirección MAC del switch tanto en el BID raíz como emisor. Estas BPDU se consideran inferiores dado que se generan en el switch designado que ha perdido su enlace con el puente raíz. El switch designado transmite las BPDU con la información de que es el puente raíz y el puente designado a la vez. Estas BPDU contienen la dirección MAC del switch tanto en el BID raíz como emisor.

Los BID se reciben en todos los switches. Cada switch reemplaza los BID de raíz más alta por BID de raíz más baja en las BPDU que se envían. Todos los switches reciben las BPDU y determinan que el switch que cuyo valor de BID raíz es el más bajo será el puente raíz.

El administrador de red puede establecer la prioridad de switch en un valor más pequeño que el del valor por defecto, lo que hace que el BID sea más pequeño.

Esto sólo se debe implementar cuando se tiene un conocimiento cabal del flujo de tráfico en la red.

4.3.1.4 Etapas de los estados del puerto Spanning Tree

Se necesita tiempo para que la información de protocolo se propague a través de una red conmutada. Los cambios de topología en una parte de la red no se conocen de inmediato en las otras partes de la red. Hay retardo de propagación. Un switch no debe cambiar el estado de un puerto de inactivo a activo de forma inmediata dado que esto puede provocar loops de datos.

Cada puerto de un switch que usa protocolo de spanning- tree se encuentra en uno de cinco estados diferentes.

En el estado de bloqueo, los puertos sólo pueden recibir las BPDU. Las tramas de datos se descartan y no se puede aprender ninguna dirección. El cambio de un estado a otro puede tardar hasta unos 20 segundos.

Los puertos pasan del estado de bloqueo al estado de escuchar. En este estado, los switches determinan si hay alguna otra ruta hacia el puente raíz. La ruta que no sea la ruta con un menor costo hacia el puente raíz vuelve al estado de bloqueo. El período de escuchar se denomina retardo de envío y dura 15 segundos. En el estado de escuchar, los datos no se envían y no se reciben las direcciones MAC. Las BPDU todavía se siguen procesando.

Los puertos pasan del estado de escuchar al estado de aprender. En este estado, los datos de usuario no se envían pero se aprenden las direcciones MAC del tráfico que se recibe. El estado de aprender dura 15 segundos y también se denomina retardo de envío. Las BPDU todavía se siguen procesando.

El puerto pasa del estado de aprender al estado de enviar. En este estado, los datos se envían y se siguen aprendiendo las direcciones MAC. Las BPDU todavía se siguen procesando.

El puerto puede estar en estado deshabilitado. Este estado deshabilitado se puede producir cuando un administrador desactiva el puerto o el puerto falla.

Los valores de tiempo determinados para cada estado son los valores por defecto. Estos valores se calculan basándose en que habrá una cantidad máxima de siete switches en cualquier rama del spanning-tree desde el puente raíz.

4.3.1.5 Recálculo de Spanning-Tree

Una internetwork conmutada converge cuando todos los puertos de switch y de puente están en estado de enviar o bloquear. Los puertos que realizan el envío envían y reciben tráfico de datos y las BPDU. Los puertos que están bloqueados sólo pueden recibir las BPDU.

Cuando la topología de red cambia, los switches y los puentes vuelven a calcular el spanning-tree y provocan una interrupción del tráfico de red. La convergencia en una nueva topología de spanning-tree que usa el estándar IEEE 802.1d puede tardar hasta 50 segundos. Esta convergencia está compuesta por una antigüedad máxima de 20 segundos, además del retardo de envío al escuchar, que es de 15 segundos, y el retardo de envío al recibir, que es de 15 segundos.

4.3.1.6 Protocolo Rapid Spanning-Tree

- El protocolo Rapid Spanning-Tree se define en el estándar de LAN IEEE 802.1w. El estándar y el protocolo presentan nuevas características: Aclaración de los estados de puerto y los roles
- Definición de un conjunto de tipos de enlace que pueden pasar rápidamente al estado enviar.
- El concepto de permitir que los switches de una red en la que hay convergencia generen las BPDU en lugar de transferir las BPDU del puente raíz.

Se ha cambiado el nombre del estado "bloqueado" por un estado de "descarte".

El rol de un puerto de descarte es el de un puerto alternativo. El puerto de descarte se puede convertir en el puerto designado si el puerto designado del segmento falla.

Los tipos de enlace se han definido como punto a punto, de extremo y compartido.
Estos cambios permiten la detección rápida de una falla de enlace en las redes conmutadas.

Los enlaces punto a punto y los enlaces de tipo de extremo pueden pasar al estado de enviar de forma inmediata.

Con estos cambios, la convergencia de red no debe tardar más de 15 segundos.

Con el tiempo, el protocolo Rapid Spanning-Tree, IEEE 802.1w reemplazará al protocolo Spanning-Tree, IEEE 802.1d.

4.3.2 CONCEPTOS GENERALES SOBRE VLANS.

4.3.2.1 Introducción a las VLAN

Una VLAN es una agrupación lógica de estaciones, servicios y dispositivos de red que no se limita a un segmento de LAN físico.

Las VLAN facilitan la administración de grupos lógicos de estaciones y servidores que se pueden comunicar como si estuviesen en el mismo segmento físico de LAN. También facilitan la administración de mudanzas, adiciones y cambios en los miembros de esos grupos.

Las VLAN segmentan de manera lógica las redes conmutadas según las funciones laborales, departamentos o equipos de proyectos, sin importar la ubicación física de los usuarios o las conexiones físicas a la red. Todas las estaciones de trabajo y servidores utilizados por un grupo de trabajo en particular comparten la misma VLAN, sin importar la conexión física o la

ubicación.

Una estación de trabajo en un grupo de VLAN se limita a comunicarse con los servidores de archivo en el mismo grupo de VLAN. Las VLAN segmentan de forma lógica la red en diferentes dominios de broadcast, de manera tal que los paquetes sólo se conmutan entre puertos y se asignan a la misma VLAN. Las VLAN se componen de hosts o equipos de red conectados mediante un único dominio de puenteo. El dominio de puenteo se admite en diferentes equipos de red. Los switches de LAN operan protocolos de puenteo con un grupo de puente separado para cada VLAN.

Las VLAN se crean para brindar servicios de segmentación proporcionados tradicionalmente por routers físicos en las configuraciones de LAN. Las VLAN se ocupan de la escalabilidad, seguridad y gestión de red. Los routers en las topologías de VLAN proporcionan filtrado de broadcast, seguridad y gestión de flujo de tráfico. Los switches no puentean ningún tráfico entre VLAN, dado que esto viola la integridad del dominio de broadcast de las VLAN. El tráfico sólo debe enrutarse entre VLAN.

4.3.2.2 Operación de las VLAN

Una VLAN se compone de una red conmutada que se encuentra lógicamente segmentada. Cada puerto de switch se puede asignar a una VLAN. Los puertos asignados a la misma VLAN comparten broadcast. Los puertos que no pertenecen a esa VLAN no comparten esos broadcast. Esto mejora el desempeño de la red porque se reducen los broadcast innecesarios. Las VLAN de asociación estática se denominan VLAN de asociación de puerto central y basadas en puerto. Cuando un dispositivo entra a la red, da por sentado automáticamente que la VLAN está asociada con el puerto al que se conecta.

Los usuarios conectados al mismo segmento compartido comparten el ancho de banda de ese segmento. Cada usuario adicional conectado al medio compartido significa que el ancho de banda es menor y que se deteriora el desempeño de la red. Las VLAN ofrecen mayor ancho de banda a los usuarios

que una red Ethernet compartida basada en hubs. La VLAN por defecto para cada puerto del switch es la VLAN de administración. La VLAN de administración siempre es la VLAN 1 y no se puede borrar. Por lo menos un puerto debe asignarse a la VLAN 1 para poder gestionar el switch. Todos los demás puertos en el switch pueden reasignarse a VLAN alternadas.

Las VLAN de asociación dinámica son creadas mediante software de administración de red. Las VLAN dinámicas permiten la asociación basada en la dirección MAC del dispositivo conectado al puerto de switch. Cuando un dispositivo entra a la red, el switch al que está conectado consulta una base de datos en el Servidor de Configuración de VLAN para la asociación de VLAN.

En la asociación de VLAN de puerto central basada en puerto, el puerto se asigna a una asociación de VLAN específica independiente del usuario o sistema conectado al puerto. Al utilizar este método de asociación, todos los usuarios del mismo puerto deben estar en la misma VLAN. Un solo usuario, o varios usuarios pueden estar conectados a un puerto y no darse nunca cuenta de que existe una VLAN.

4.3.2.3 Ventajas de las VLAN

Las VLAN permiten que los administradores de red organicen las LAN de forma lógica en lugar de física. Ésta es una ventaja clave. Esto permite que los administradores de red realicen varias tareas:

- Trasladar fácilmente las estaciones de trabajo en la LAN
- Agregar fácilmente estaciones de trabajo a la LAN
- Cambiar fácilmente la configuración de la LAN
- Controlar fácilmente el tráfico de red
- Mejorar la seguridad

4.3.2.4 Tipos de VLAN

En esta página se describen tres asociaciones básicas de VLAN que se utilizan para determinar y controlar de qué manera se asigna un paquete:

- VLAN basadas en puerto
- VLAN basadas en direcciones MAC
- VLAN basadas en protocolo

La cantidad de VLAN en un switch varía según diversos factores:

- Patrones de tráfico
- Tipos de aplicaciones
- Necesidades de administración de red
- Aspectos comunes del grupo

El esquema de direccionamiento IP es otra consideración importante al definir la cantidad de VLAN en un switch.

Por ejemplo, una red que usa una máscara de 24 bits para definir una subred tiene en total 254 direcciones de host permitidas en una subred. Dado que es altamente recomendada una correspondencia de uno a uno entre las VLAN y las subredes IP, no puede haber más de 254 dispositivos en una VLAN. También se recomienda que las VLAN no se extiendan fuera del dominio de Capa 2 del switch de distribución.

Existen dos métodos principales para el etiquetado de tramas: el enlace Inter-Switch (ISL) y 802.1Q. ISL es un protocolo propietario de Cisco y antiguamente era el más común, pero está siendo reemplazado por el etiquetado de trama

estándar IEEE 802.1Q [4].

A medida que los paquetes son recibidos por el switch desde cualquier dispositivo de estación final conectado, se agrega un identificador único de paquetes dentro de cada encabezado. Esta información de encabezado designa la asociación de VLAN de cada paquete. El paquete se envía entonces a los switches o routers correspondientes sobre la base del identificador de VLAN y la dirección MAC. Al alcanzar el nodo destino, el ID de VLAN es eliminado del paquete por el switch adyacente y es enviado al dispositivo conectado. El etiquetado de paquetes brinda un mecanismo para controlar el flujo de broadcast y aplicaciones, mientras que no interfiere con la red y las aplicaciones.

[4] ANSI/IEEE Standard 802.1Q, "IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks", 1998.

5. MPLS (Multiprotocol Label Switching)

5.1 Introducción a MPLS

Durante el tiempo en que se ha desarrollado el estándar, se han extendido algunas ideas falsas o inexactas sobre el alcance y objetivos de MPLS. Inicialmente se pensaba que MPLS se había desarrollado para ofrecer un estándar a los vendedores que les permitiese evolucionar los conmutadores ATM a *routers* de *backbone* de altas prestaciones.

Aunque esta puede haber sido la finalidad original de los desarrollos de conmutación multinivel, los recientes avances en tecnologías de silicio ASIC permiten a los *routers* funcionar con una rapidez similar para la consulta de tablas a las de los conmutadores ATM. Si bien es cierto que MPLS mejora notablemente el rendimiento del mecanismo de envío de paquetes, éste no era el principal objetivo del grupo del IETF.

Los objetivos establecidos por ese grupo en la elaboración del estándar eran:

- MPLS debía funcionar sobre cualquier tecnología de transporte, no sólo ATM.
- MPLS debía soportar el envío de paquetes tanto unicast como multicast.
- MPLS debía ser compatible con el Modelo de Servicios Integrados del IETF, Incluyendo el protocolo RSVP8.
- MPLS debía permitir el crecimiento constante de la Internet.
- MPLS debía ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP.

Se pensaba también que MPLS perseguía eliminar totalmente el encaminamiento convencional por prefijos de red. Esta es otra idea falsa y nunca se planteó como objetivo del grupo, ya que el encaminamiento tradicional de nivel 3 siempre sería un requisito en la Internet por los siguientes motivos:

· El filtrado de paquetes en los Firewalls (FW) de acceso a las LAN corporativas y en los límites de las redes de los NSPs es un requisito fundamental para poder gestionar la red y los servicios con las necesarias garantías de seguridad. Para ello se requiere examinar la información de la cabecera de los paquetes, lo que impide prescindir del uso del nivel 3 en ese tipo de aplicaciones.

· No es probable que los sistemas finales (*hosts*) implementen MPLS. Necesitan enviar los paquetes a un primer dispositivo de red (nivel 3) que pueda examinar la cabecera del paquete para tomar luego las correspondientes decisiones sobre su envío hasta su destino final. En este primer salto se puede decidir enviarlo por *routing* convencional o asignar una etiqueta y enviarlo por un LSP.

· Las etiquetas MPLS tienen solamente significado local (es imposible mantener vínculos globales entre etiquetas y *hosts* en toda la Internet). Esto implica que en algún punto del camino algún dispositivo de nivel 3 debe examinar la cabecera del paquete para determinar con exactitud por dónde lo envía: por *routing* convencional o entregándolo a un LSR, que lo expedirá por un nuevo LSP.

· Del mismo modo, el último LSR de un LSP debe usar encaminamiento de nivel 3 para entregar el paquete al destino, una vez suprimida la etiqueta, como se verá seguidamente al describir la funcionalidad MPLS.

5.2 Descripción funcional de MPLS

La operación del MPLS se basa en las componentes funcionales de envío y control, aludidas anteriormente, y que actúan ligadas íntimamente entre sí.

5.2.1 Funcionamiento del envío de paquetes en MPLS

La base del MPLS está en la asignación e intercambio de etiquetas, que permiten el establecimiento de los caminos LSP por la red. Los LSPs son simplex por naturaleza (se establecen para un sentido del tráfico en cada punto de entrada a la red); para el tráfico dúplex requiere dos LSPs, uno en cada sentido. Cada LSP se crea a base de concatenar uno o más saltos (*hops*) en los que se intercambian las etiquetas, de modo que cada paquete se envía de un "conmutador de etiquetas" (*Label-Swiching Router)* a otro, a través del dominio MPLS. Un LSR no es sino un router especializado en el envío de paquetes etiquetados por MPLS.

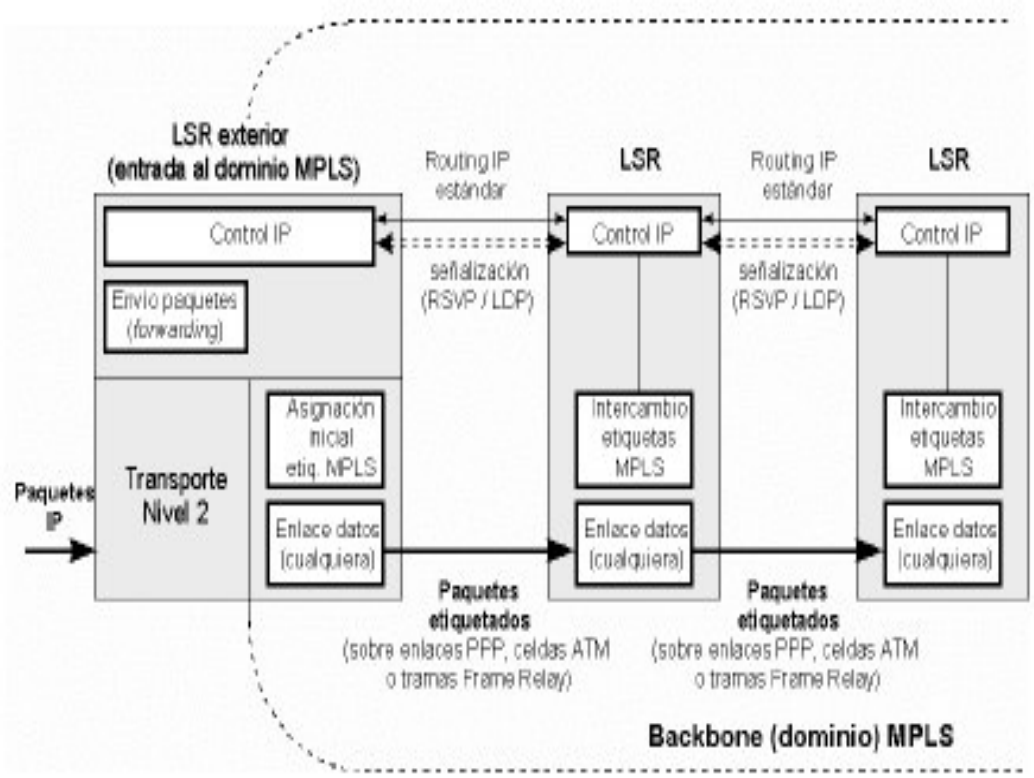

fig. 6

MPLS no utiliza ninguno de los protocolos de señalización ni de encaminamiento definidos por el ATM Forum; en lugar de ello, en MPLS o bien se utiliza el protocolo RSVP o bien un nuevo estándar de señalización (el *Label Distribution Protocol*, LDP, del que se tratará más adelante). Pero, de acuerdo con los requisitos del IETF, el transporte de datos puede ser cualquiera. Si éste fuera ATM, una red IP habilitada para MPLS es ahora mucho más sencilla de gestionar que la solución clásica IP/ATM. Ahora ya no hay que administrar dos arquitecturas diferentes a base de transformar las direcciones IP y las tablas de encaminamiento en las direcciones y el encaminamiento ATM: esto lo resuelve el procedimiento de intercambio de etiquetas MPLS. El papel de ATM queda restringido al mero transporte de datos basado en celdas. Para MPLS esto es indiferente, ya que puede utilizar otros transportes como Frame Relay, o directamente sobre líneas punto a punto.

Un camino LSP es el circuito virtual que siguen por la red todos los paquetes asignados a la misma FEC. Al primer LSR que interviene en un LSP se le denomina de entrada o de cabecera y al último se le denomina de salida o de cola. Los dos están en el exterior del dominio MPLS. El resto, entre ambos, son LSRs interiores del dominio MPLS. Un LSR es como un router que funciona a base de intercambiar etiquetas según una tabla de envío. Esta tabla se construye a partir de la información de encaminamiento que proporciona la componente de control (recuérdese el esquema de la figura 6), según se verá más adelante. Cada entrada de la tabla contiene un par de etiquetas entrada/salida correspondientes a cada interfaz de entrada, que se utilizan para acompañar a cada paquete que llega por esa interfaz y con la misma etiqueta (en los LSR exteriores sólo hay una etiqueta, de salida en el de cabecera y de entrada en el de cola). En la figura 7 se ilustra un ejemplo del funcionamiento de un LSR del núcleo MPLS. A un paquete que llega al LSR por la interfaz 3 de entrada con la etiqueta 45 el LSR le asigna la etiqueta 22 y lo envía por el interfaz 4 de salida al siguiente LSR, de acuerdo con la información de la tabla.

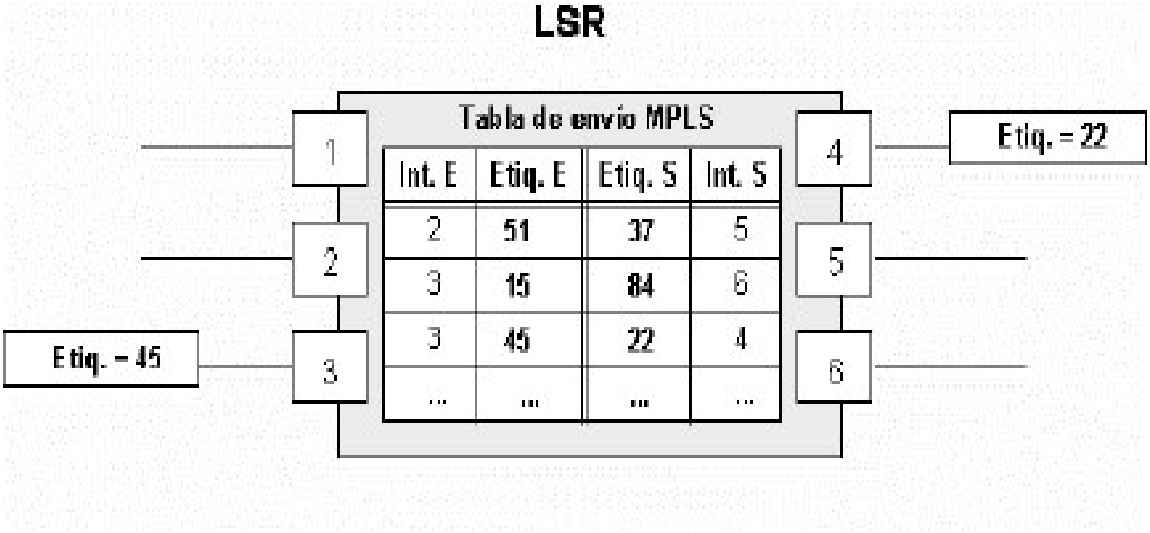

fig. 7

El algoritmo de intercambio de etiquetas requiere la clasificación de los paquetes a la entrada del dominio MPLS para poder hacer la asignación por el LSR de cabecera.

5.2.2 Control de la información en MPLS

Hasta ahora se ha visto el mecanismo básico de envío de paquetes a través de los LSPs mediante el procedimiento de intercambio de etiquetas según las tablas de los LSRs. Pero queda por ver dos aspectos fundamentales:

1. Cómo se generan las tablas de envío que establecen los LSPs.
2. Cómo se distribuye la información sobre las etiquetas a los LSRs.

El primero de ellos está relacionado con la información que se tiene sobre la red: topología, patrón de tráfico, características de los enlaces, etc. Es la información de control típica de los algoritmos de encaminamiento. MPLS necesita esta información de *routing* para establecer los caminos virtuales LSPs. Lo más lógico es utilizar la propia información de encaminamiento que manejan los protocolos internos IGP (OSPF, IS-IS, RIP...) para construir las tablas de encaminamiento (recuérdese que los LSR son *routers* con funcionalidad añadida). Esto es lo que hace MPLS precisamente: para cada

"ruta IP" en la red se crea un "camino de etiquetas" a base de concatenar las de entrada/salida en cada tabla de los LSRs; el protocolo interno correspondiente se encarga de pasar la información necesaria.

El segundo aspecto se refiere a la información de "señalización", pero siempre que se quiera establecer un circuito virtual se necesita algún tipo de señalización para marcar el camino, es decir, para la distribución de etiquetas entre los nodos. Sin embargo, la arquitectura MPLS no asume un único protocolo de distribución de etiquetas; de hecho se están estandarizando algunos existentes con las correspondientes extensiones; unos de ellos es el protocolo RSVP del Modelo de Servicios Integrados del IETF (recuérdese que ése era uno de los requisitos). Pero, además, en el IETF se están definiendo otros nuevos, específicos para la distribución de etiquetas, cual es el caso del *Label Distribution Protocol* (LDP).

5.2.3 Funcionamiento global MPLS

Una vez vistos todos los componentes funcionales, el esquema global de funcionamiento es el que se muestra en la figura 8, donde quedan reflejadas las diversas funciones en cada uno de los elementos que integran la red MPLS. Es importante destacar que en el borde de la nube MPLS tenemos una red convencional de *routers* IP. El núcleo MPLS proporciona una arquitectura de transporte que hace aparecer a cada par de *routers* a una distancia de un sólo salto. Funcionalmente es como si estuvieran unidos todos en una topología mallada (directamente o por PVCs ATM). Ahora, esa unión a un solo salto se realiza por MPLS mediante los correspondientes LSPs (puede haber más de uno para cada par de *routers*). La diferencia con topologías conectivas reales es que en MPLS la construcción de caminos virtuales es mucho más flexible y que no se pierde la visibilidad sobre los paquetes IP. Todo ello abre enormes posibilidades a la hora de mejorar el rendimiento de las redes y de soportar nuevas aplicaciones de usuario, tal como se explica en la sección siguiente.

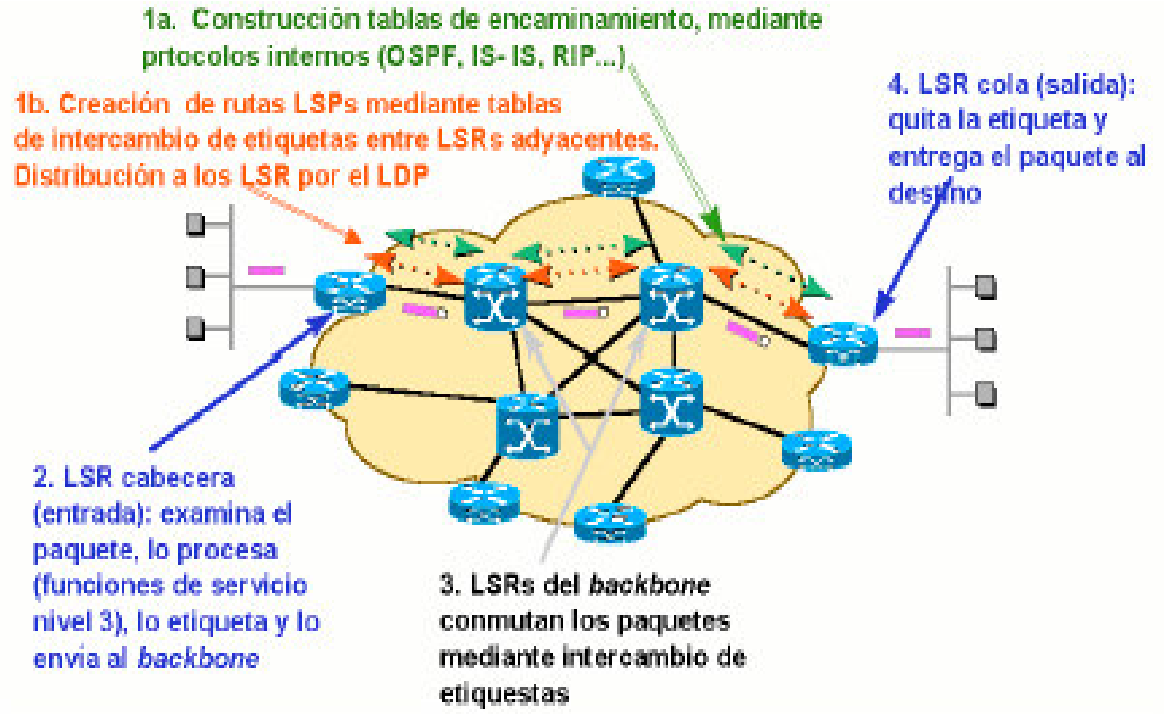

fig. 8

5.3 Aplicaciones de MPLS

Las principales aplicaciones que hoy en día tiene MPLS son:

- Ingeniería de tráfico.
- Diferenciación de niveles de servicio mediante clases (CoS).
- Servicio de redes privadas virtuales (VPN).

Veamos brevemente las características de estas aplicaciones y las ventajas que MPLS supone para ello frente a otras soluciones tradicionales.

5.3.1 Ingeniería de tráfico

El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los Recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera que no haya algunos que estén suprautilizados, con posibles puntos calientes y cuellos de botella, mientras otros puedan estar infrautilizados. A comienzos de los 90 los esquemas para adaptar de forma

efectiva los flujos de tráfico a la topología física de las redes IP eran bastante rudimentarios. Los flujos de tráfico siguen el camino más corto calculado por el algoritmo IGP correspondiente. En casos de congestión de algunos enlaces, el problema se resolvía a base de añadir más capacidad a los enlaces. La ingeniería de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo IGP sobre enlaces más congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta (con menos saltos).

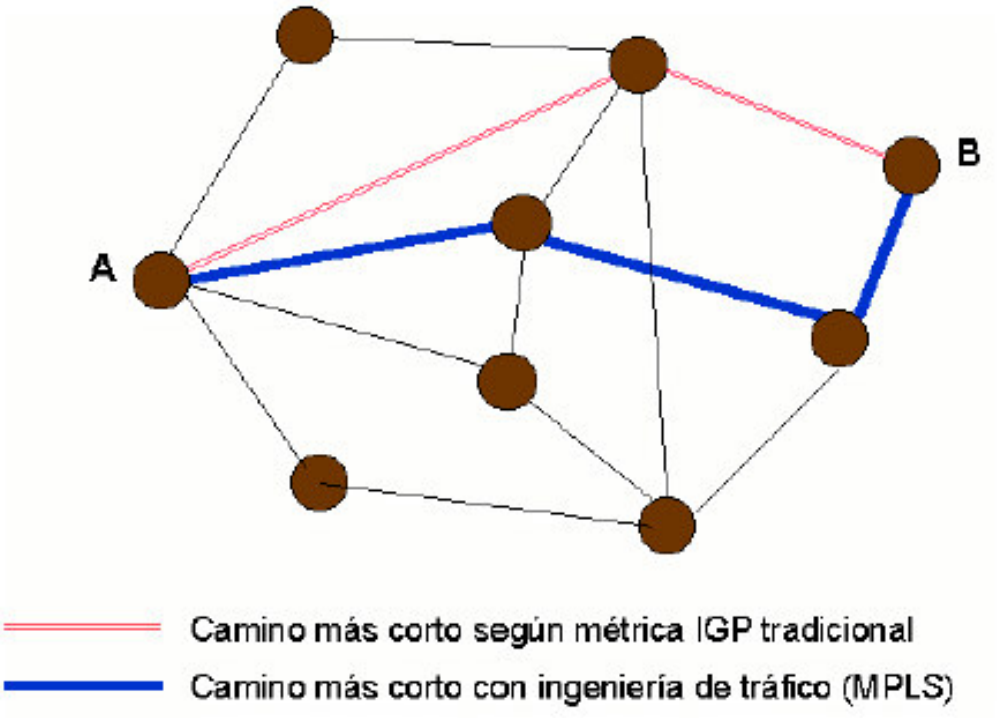

fig. 9

El camino más corto entre A y B según la métrica normal IGP es el que tiene sólo dos saltos, pero puede que el exceso de tráfico sobre esos enlaces o el esfuerzo de los routers correspondientes haga aconsejable la utilización del camino alternativo indicado con un salto más. MPLS es una herramienta efectiva para esta aplicación en grandes *backbones*, ya que:

· Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.

· Permite obtener estadísticas de uso LSP, que se pueden utilizar en la planificación de la red y como herramientas de análisis de cuellos de botella y

carga de los enlaces, lo que resulta bastante útil para planes de expansión futura.

· Permite hacer "encaminamiento restringido" (*Constraint-based Routing*, CBR), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales (distintos niveles de calidad). Por ejemplo, con garantías explícitas de retardo, ancho de banda, fluctuación, pérdida de paquetes, etc.

La ventaja de la ingeniería de tráfico MPLS es que se puede hacer directamente sobre una red IP, al margen de que haya o no una infraestructura ATM por debajo, todo ello de manera más flexible y con menores costes de planificación y gestión para el administrador, y con mayor calidad de servicio para los clientes.

5.3.2 Clases de Servicio (CoS)

MPLS está diseñado para poder cursar servicios diferenciados, según el Modelo DiffServ del IETF. Este modelo define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio, con diferentes prioridades. Según los requisitos de los usuarios, DiffServ permite diferenciar servicios tradicionales tales como el WWW, el correo electrónico o la transferencia de ficheros (para los que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de video y voz interactiva. Para ello se emplea el campo ToS (*Type of Service*), rebautizado en DiffServ como el octeto DS. Esta es la técnica QoS de marcar los paquetes que se envían a la red.

MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP.

De este modo, una red MPLS puede transportar distintas clases de tráfico, ya que:

· El tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP.

· Entre cada par de LSR exteriores se pueden provisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda. P. Ej., un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico *best-effort*, tres niveles de servicio, primero, preferente y turista, que, lógicamente, tendrán distintos precios.

5.3.3 Redes Privadas Virtuales (VPNs)

Una red privada virtual (VPN) se construye basado en conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada. El objetivo de las VPNs es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos y video sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad supone aislamiento, y "privada" indica que el usuario "cree" que posee los enlaces. Las IP VPNs son soluciones de comunicación VPN basada en el protocolo de red IP de la Internet. En esta sección se va a describir brevemente las ventajas que MPLS ofrece para este tipo de redes frente a otras soluciones tradicionales.

Las VPNs tradicionales se han venido construyendo sobre infraestructuras de transmisión compartidas con características implícitas de seguridad y respuesta Predeterminada. Tal es el caso de las redes de datos Frame Relay, que permiten establecer PVCs entre los diversos nodos que conforman la VPN. La seguridad y las garantías las proporcionan la separación de tráficos por PVC y el caudal asegurado (CIR). Algo similar se puede hacer con ATM, con diversas clases de garantías. Los inconvenientes de este tipo de solución es que la configuración de las rutas se basa en procedimientos más bien artesanales, al tener que establecer cada PVC entre nodos, con la complejidad que esto supone al proveedor en la gestión (y los mayores costes asociados). Si se quiere tener conectados a todos con todos, en una topología lógica totalmente mallada, añadir un nuevo emplazamiento supone retocar todos los CPEs del cliente y restablecer todos los PVCs.

Además, la popularización de las aplicaciones TCP/IP, así como la expansión de las redes de los NSPs, ha llevado a tratar de utilizar estas infraestructuras IP para el soporte de VPNs, tratando de conseguir una mayor flexibilidad en el

diseño e implantación y unos menores costes de gestión y provisión de servicio. La forma de utilizar las infraestructuras IP para servicio VPN (IP VPN) ha sido la de construir túneles IP de diversos modos.

El objetivo de un túnel sobre IP es crear una asociación permanente entre dos extremos, de modo que funcionalmente aparezcan conectados. Lo que se hace es utilizar una estructura no conectiva como IP para simular esas conexiones: una especie de tuberías privadas por las que no puede entrar nadie que no sea miembro de esa IP VPN. No es el objetivo de esta sección una exposición completa de IP VPNs sobre túneles; se pretende tan sólo resumir sus características para poder apreciar luego las ventajas que ofrece MPLS frente a esas soluciones.

Los túneles IP en conexiones dedicadas se pueden establecer de dos maneras:

· En el nivel 3, mediante el protocolo IPSec10 del IETF.

· En el nivel 2, mediante el encapsulamiento de paquetes privados (IP u otros) Sobre una red IP pública de un NSP.

En las VPNs basadas en túneles IPSec, la seguridad requerida se garantiza mediante el cifrado de la información de los datos y de la cabecera de los paquetes IP, que se encapsulan con una nueva cabecera IP para su transporte por la red del proveedor. Es relativamente sencillo de implementar, bien sea en dispositivos especializados, tales como firewalls, como en los propios *routers* de acceso del NSP. Además, como es un estándar, IPSec permite crear VPNs a través de redes de distintos NSPs que sigan el estándar IPSec. Pero como el cifrado IPSec oculta las cabeceras de los paquetes originales, las opciones QoS son bastante limitadas, ya que la red no puede distinguir flujos por aplicaciones para asignarles diferentes niveles de servicio. Además, sólo vale para paquetes IP nativos, IPSec no admite otros protocolos.

En los túneles de nivel 2 se encapsulan paquetes multiprotocolo (no necesariamente IP), sobre los datagramas IP de la red del NSP. De este modo, la red del proveedor no pierde la visibilidad IP, por lo que hay mayores posibilidades de QoS para priorizar el tráfico por tipo de aplicación IP. Los clientes VPN pueden mantener su esquema privado de direcciones, estableciendo grupos cerrados de usuarios, si así lo desean. (Además de encapsular los paquetes, se puede cifrar la información por mayor seguridad,

pero en este caso limitando las opciones QoS). A diferencia de la opción anterior, la operación de túneles de nivel 2 está condicionada a un único proveedor.

A pesar de las ventajas de los túneles IP sobre los PVCs, ambos enfoques tienen unas características comunes que las hacen menos eficientes frente a la solución MPLS:

· Están basadas en conexiones punto a punto (PVCs o túneles).

· La configuración es manual.

· La provisión y gestión son complicadas; una nueva conexión supone alterar todas las configuraciones.

· Plantean problemas de crecimiento al añadir nuevos túneles o circuitos virtuales.

· La gestión de QoS es posible en cierta medida, pero no se puede mantener extremo a extremo a lo largo de la red, ya que no existen mecanismos que sustenten los parámetros de calidad durante el transporte. Realmente, el problema que plantean estas IP VPNs es que están basadas en un *modelo topológico superpuesto* sobre la topología física existente, basados en túneles extremos a extremo (o circuitos virtuales) entre cada par de *routers* de cliente en cada VPN. De ahí las desventajas en cuanto a la poca flexibilidad en la provisión y gestión del servicio, así como en el crecimiento cuando se quieren añadir nuevos emplazamientos. Con una arquitectura MPLS se obvian estos inconvenientes ya que el modelo topológico no se superpone sino que se acopla a la red del proveedor. En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una "nube común" en las que solamente pueden entrar los miembros de la misma VPN. Las "nubes" que representan las distintas VPNs se implementan mediante los caminos LSPs creados por el mecanismo de intercambio de etiquetas MPLS. Los LSPs son similares a los túneles en cuanto a que la red transporta los paquetes del usuario (incluyendo las cabeceras) sin examinar el contenido, a base de encapsularlos sobre otro protocolo. Aquí está la diferencia: en los túneles se utiliza el encaminamiento convencional IP para transportar la información del usuario, mientras que en MPLS esta información se transporta sobre el mecanismo de intercambio de etiquetas, que no ve para nada el proceso de *routing* IP. Sin embargo, sí se

mantiene en todo momento la visibilidad IP hacia el usuario, que no sabe nada de rutas MPLS sino que ve un internet privado (intranet) entre los miembros de su VPN. De este modo, se pueden aplicar técnicas QoS basadas en el examen de la cabecera IP, que la red MPLS podrá propagar hasta el destino, pudiendo así reservar ancho de banda, priorizar aplicaciones, establecer CoS y optimizar los recursos de la red con técnicas de ingeniería de tráfico.

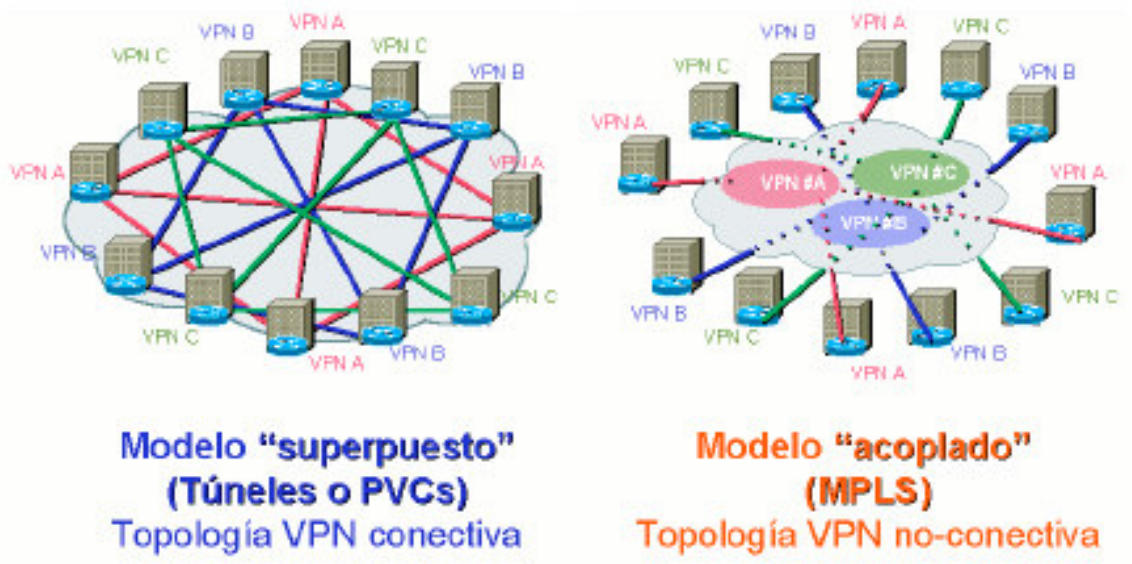

fig. 10

En la figura 10 se representa una comparación entre ambos modelos. La diferencia entre los túneles IP convencionales (o los circuitos virtuales) y los "túneles MPLS" (LSPs) está en que éstos se crean *dentro de la red*, basados en LSPs, y no de extremo a extremo *a través de la red.*

Como resumen, las ventajas que MPLS ofrece para IP VPNs son:

· Proporcionan un modelo "acoplado" o "inteligente", ya que la red MPLS "sabe" de la existencia de VPNs (lo que no ocurre con túneles ni PVCs).

· Evita la complejidad de los túneles y PVCs.

· La provisión de servicio es sencilla: una nueva conexión afecta a un solo *router* tiene mayores opciones de crecimiento modular.

· Permiten mantener garantías QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias al vínculo que

mantienen el campo EXP de las etiquetas MPLS con las clases definidas a la entrada.

· Permite aprovechar las posibilidades de ingeniería de tráfico para poder garantizar los parámetros críticos y la respuesta global de la red (ancho banda, retardo, fluctuación...), lo que es necesario para un servicio completo VPN [5].

[5] Monografía MPLS conmutación de etiquetas Multiprotocolo 2004.

6. VPLS (Virtual Private Lan Service).

6.1 Introducción a VPLS y Seudocables Martíni.

Los seudocables Martini proporcionan las capacidades adicionales de separación de tráfico entre los clientes y multiplexan flujos de diferentes clientes en túneles de transporte para obtener una conectividad de punto a punto. Los túneles de transporte se establecen con RSVP-TE o LDP. Los circuitos de clientes se establecen por medio de LDP dirigido a proveer la separación del tráfico entre dos extremos de un Operador.

VPLS permite la conectividad multipunto y habilita los servicios LAN a LAN, al proporcionar un dominio de transmisión por cliente, como si todos los sitios (el borde del cliente o CE) estuvieran conectados a la misma LAN. Todos los routers de borde del Operador (PE) se interconectan entre sí para proporcionar conectividad de sitio a sitio sin tener que ejecutar el protocolo de árbol en expansión para evitar loops. El tráfico multicast se trata como tráfico de transmisión general broadcast y por lo tanto, se replica por todos los puertos que pertenecen a una instancia específica de cliente.

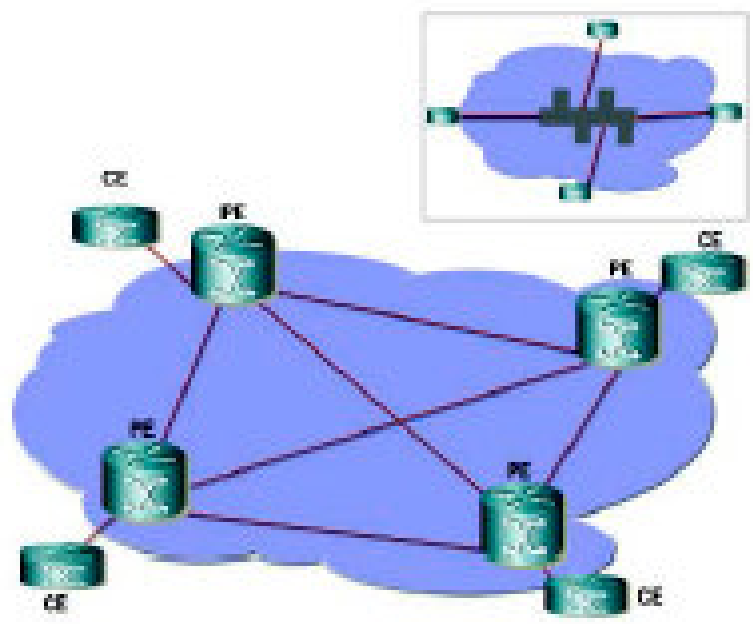

fig. 11

VPLS, la red es un solo dominio de Broadcast como se representa en la imagen más pequeña de la figura 11.

Los requisitos de malla completa y replicación imponen límites en cuanto al número total de PE VPLS que se pueden conectar dentro de un solo dominio de VPLS. Cuando el número total de PEs alcance 40-60, se recomienda crear una jerarquía de niveles múltiples para escalar los servicios VPLS (descritos a continuación). En el año 2002, Riverstone lanzó los primeros routers habilitados para Martini y VPLS.

Es importante poder conectar las interfaces antiguas, como ATM o Frame Relay además de los puertos Ethernet, debido a que estas tecnologías todavía se pueden usar de manera transparente como interfaces de acceso a MPLS / VPLS. En el caso de Ethernet, el acondicionamiento de tráfico (como la limitación de velocidad y la conformación o shaping) proporciona capacidades similares en términos de QoS y fraccionamiento del ancho de banda que las de los circuitos virtuales ATM y Frame Relay. Posteriormente, cada circuito se vincula a un LSP de circuito virtual (VC) basado en el puerto entrante, VLAN o rango de VLAN. Este proceso se conoce como búsqueda FEC (Forwarding Equivalence Class). Las etiquetas 802.1p se pueden usar para clasificar el tráfico en los LSPs apropiados y para marcar los bits EXP MPLS correspondientes. El programador (scheduler) de tramas usa dichas marcas para proporcionar una calidad de servicio diferenciada (DiffServ QoS) ante una contienda por recursos.

Los nuevos desarrollos en el plano tecnológico de empresas como CISCO y Riverstone han permitido obtener productos como la nueva versión del sistema operativo (RapidOS) que permite buscar los códigos de punto de DSCP especificados en el encabezado IP de los paquetes del cliente, a fin de identificar la cola de espera, el algoritmo de programación (scheduling) y el marcado de tramas que se van a aplicar; Los routers también se han mejorado para los clientes que requieren CPEs con conexión redundante (dual homed). Además de activar el protocolo de Árbol en expansión entre los sitios del cliente y los PEs, también es posible habilitar un mecanismo de detección de lazo (loop) único que no requiere el uso del STP para evitar lazos (loops). En el último caso, los cambios de direcciones MAC se monitorean por instancia de

puerto o de VLAN y cuando se llega a un umbral específico, se bloquean los puertos correspondientes.

La capacidad para limitar el número total de direcciones MAC que se pueden aprender en un puerto o VLAN evita que un solo cliente o un ataque de negación de servicio agote las tablas MAC VPLS.

6.1.1 OPERACIONES SOBRE REDES VPLS.

En lo que se refiere a la verificación y aislamiento de fallas, las primeras funciones disponibles son las facilidades de ping y traceroute del LSP. Estas herramientas se usan a solicitud durante la localización de fallas. Cuando un LSP no entrega tráfico, el plano de control de MPLS no siempre puede detectar la falla. La facilidad de ping del LSP (modelado con base a la solicitud / respuesta de eco del ICMP) se usa para verificar que los paquetes que correspondan a una Clase de Envío Equivalente (FEC) particular realmente terminen su trayectoria MPLS en un LSR que sea una salida para esa FEC. El paquete Traceroute se envía al plano de control de cada LSR de tránsito, el cual verifica varias veces que realmente sea un LSR de tránsito para esta trayectoria; este LSR también regresa más información que ayuda a comprobar el plano de control comparándolo con el plano de datos, es decir, que el envío corresponda con lo que los protocolos de enrutamiento determinaron como la trayectoria.

6.1.2 APROVISIONAMIENTO DE REDES VPLS.

Para establecer una red VPLS es necesario realizar las siguientes tareas:

• Conectar el dispositivo CE al dispositivo PE.

• Configurar los dispositivos PE para el nuevo servicio:

• Crear interfaces IP – En el nodo PE es necesario configurar todos los puertos Conectados a la red con las direcciones IP apropiadas.

• Crear interfaces de lazo de retorno (loopback) o ID de nodo por PE.

• Configurar un protocolo IGP (como OSPF) para el intercambio de rutas con el resto de Los PEs en la dorsal.

• Agregar interfaces a la LDP y RSVP.

• Configurar la interfaz de túneles entre todos los PEs para establecer los LSPs.
• Establecer una malla de túneles LSP.
• Definir las instancias VPLS en cada caja:
• Establecer un perfil del cliente o asignar un tipo de FEC que puede estar basada en:
• Puerto-VLAN
• Puerto
• Rango de puertos VLAN
• Rango de VLAN
• VLAN
• Conectar el perfil del cliente a su par LDP, lo que crea circuitos virtuales desde la interfaz de cliente hasta el par LDP del extremo lejano (lo mismo aplica en la dirección inversa).

6.2 ARQUITECTURAS, PROTOCOLOS Y SEÑALIZACIÒN DE MPLS/VPLS.

Estudiando dentro del IETF los distintos grupos que tocan este tema encontramos fundamentalmente dos:

· IETF Provider Provisioned Virtual Private Networks (ppvpn).
· IETF Pseudo Wire Emulation Edge to Edge (pwe3).

Ambos grupos realizan un enfoque diferente del problema. Mientras que el primero intenta identifica el esquema general del problema y el marco donde caerán las distintas soluciones (incluyendo los elementos a diseñar), el segundo se preocupa de implementar pseudo-cables de forma simular un link o un circuito (según sea el caso); es decir que estamos hablando de cómo se transportarían los PDU que ingresan a un puerto lógico para llegar al puerto de destino atravesando una nube que puede ser MPLS, IP, etc.
Como caso particular de estudio del grupo ppvpn encontramos el trabajo en VPLS: Virtual Private Lan Services, donde se destacan los aspectos generales para la configuración de una red LAN sobre un Backbone MPLS. A su vez el grupo pwe3 ha trabajado en el transporte de tramas Ethernet sobre MPLS.

6.2.1 Marco General para VPLS.

El requerimiento a cumplir consiste en la emulación de una red LAN sobre infraestructura IP/MPLS, a éste servicio se lo denomina VPLS.

Definiciones:

VPLS: Virtual Private Lan Service: Es una implementación de VPN de nivel 2 caracterizado por el soporte de difusión de capa 2. Todos los clientes de un servicio VPLS pertenecerán a una misma LAN sin importar su ubicación.

Dominio VPLS: Está formado por una comunidad de interés de direcciones MAC y VLANs. Un sólo dominio puede tener varias VLANs en él.

VSI: Virtual Switching Instance: Es la entidad de capa 2 que está más próxima a un miembro de un dominio VPLS. Puede basarse en direcciones MAC, etiqueta de VLAN, parámetros de QoS, entre otros. En la figura 12 se muestra el modelo de referencia sobre el cuál se basa la arquitectura de VPLS.

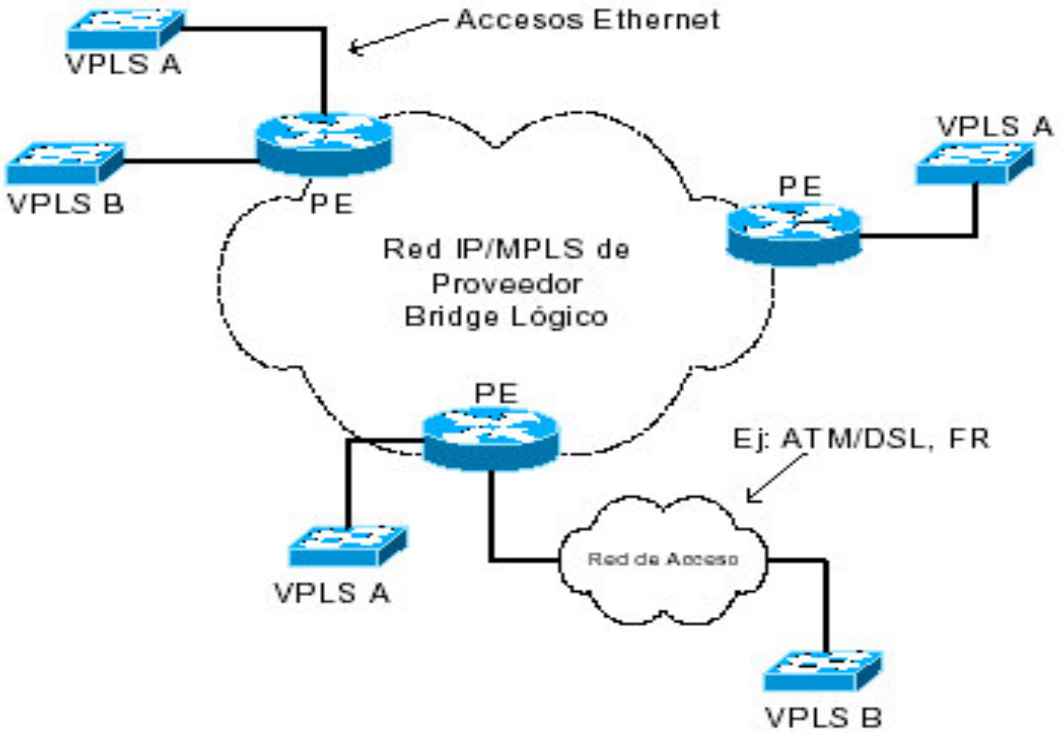

fig. 12

Modelo de referencia para VPLS, la red del proveedor actual como un gran bridge transparente virtual.

Al igual que en el caso de VPN de nivel 3 donde son los equipos PE quienes realizan la clasificación de los paquetes, estos mismos equipos van a mantener los dominios de difusión de cada VPLS y mapear a éstos en sus correspondientes túneles.
La topología VPLS está caracterizada por lo tanto por los túneles PE-PE, estos pueden construirse según diferentes opciones:

- Punto a punto.
- Punto – multipunto.
- mallado completo.
- mallado parcial.
- Jerárquico.

Sin importar la topología escogida debe mantenerse la conectividad entre todos los clientes LAN del servicio.

Existen diferentes implementaciones para la comunicación entre los PE y los CE, como ser Ethernet pura, Frame Relay (RFC 1490), ATM (RFC 1483), pero siempre se deben utilizar tramas Ethernet como unidad de datos.
Es importante destacar que un proveedor puede tener varios accesos de diferentes servicios en una misma interfaz física, la norma prevé que en este caso la clasificación de los accesos debe ser hecho por el proveedor y no por el cliente, en la figura 13 se muestra el caso de separación de servicios utilizando una interfaz con separación por etiqueta 802.1q.

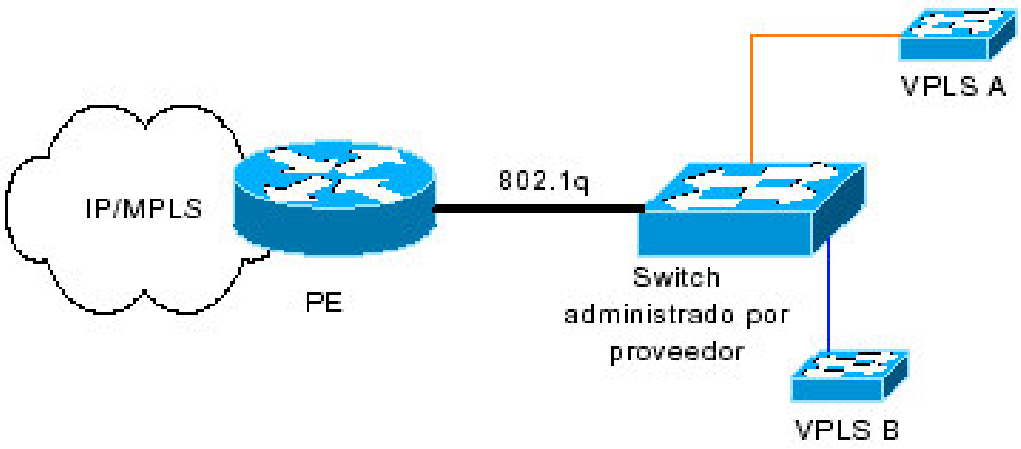

fig. 13

Se muestra el ejemplo en una interfaz ethernet donde varios dominios VPLS comparten un medio físico, la norma prevé que la clasificación la debe realizar el proveedor, por ello éste debe administrar el switch señalado.

Con respecto al plano de control, es necesario implementar mecanismos para que la operación sea transparente del protocolo de control del usuario, además de evitar la existencia de loops (por ejemplo utilizando el protocolo Spanning Tree). Se debe buscar también que el tráfico de control, así como el uso de recursos por parte del plano de control crezca linealmente con el número de clientes.

En lo que se refiere al plano de datos se busca que todo el dominio VPLS funcione como un gran bridge transparente, donde las tramas unicast de destinatario conocido sea enviado sólo a este y las tramas de difusión, multicast y unicast con destinatario desconocido sean enviadas por difusión a todos los clientes dentro del dominio VPLS. Si los equipos PE pueden comprender la información de VLAN, se podrá mantener un dominio de difusión diferente por VLAN correspondiente a cada dominio VPLS. Como todo bridge transparente cada PE va a aprender la ubicación de los clientes observando la mac de las tramas que arriban. Hay que destacar que ya en el documento a normalizar se comenta que en los servicios VPLS es necesario acotar el número de clientes LAN, ya sea con pocos sitios conectados o con pocos clientes por sitio.

En lo referente al tamaño de MTU, el mismo debe ser de al menos 1500 bytes (puede ser mayor en especial si se dan accesos de Gigabit Ethernet donde existen tramas jumbo o si es necesario considerar el encabezado 802.1q) y el servicio no debe fragmentar los paquetes generados a través de éstos servicios. Diferentes VPLS pueden tener diferentes MTU y si se soportan VLANs, dentro de un dominio VPLS, todas deben tener el mismo MTU.
Un punto interesante que se propone es la posibilidad de realizar traducciones de etiqueta de VLANs entre el PE de entrada y el de salida, de esta forma sitios remotos pueden compartir un dominio de difusión aunque tengan identificadores de VLAN locales diferentes (facilitando la interconexión de sitios con entidades de administración independientes) a este servicio se denomina extranet de nivel 2.

También se plantea la posibilidad de integración de los servicios VPLS con otros servicios contratados por el cliente como ser acceso a la infraestructura VPN de nivel 3, redes de almacenamiento entre otros.

Encapsulamiento de Tramas Ethernet sobre Redes IP/MPLS:
Como ya fue mencionado, si bien aún no existe estandarización propuesta para la implementación completa de un servicio VPLS, si existen propuestas para solucionar la conexión entre dos puntos a través de tramas ethernet pasando por una red IP/MPLS.
Básicamente se habla de implementar un pseudo-cable de nivel 2 donde en [6] se dan los requerimientos generales para diferentes protocolos y en [7] se habla específicamente de tramas ethernet. Esta implementación entra en lo denominado AToM (Any Transport over MPLS).
Como modelo de referencia en esta sección tomamos la figura 14, donde se destacan únicamente dos PE. Tomamos al equipo PE1, como el equipo de ingreso de tramas y al equipo PE2 como equipo de egreso. Como fue mencionado en la sección anterior el transporte de información entre PE1 y

[6] "Transport of Layer 2 Frames Over MPLS", Martini, L., et al., draft-ietf-pwe3-controlprotocol-01.txt, Noviembre 2002.
[7] "Encapsulation Methods for Transport of Ethernet Frames Over IP/MPLS Networks" Martini, L., et al., draft-ietf-pwe3-ethernet-encap-01.txt, Noviembre 2002.

PE2 se realiza a través de un túnel, para el caso de una red MPLS esto es un LSP, al que vamos a denominar “Túnel PSN”.

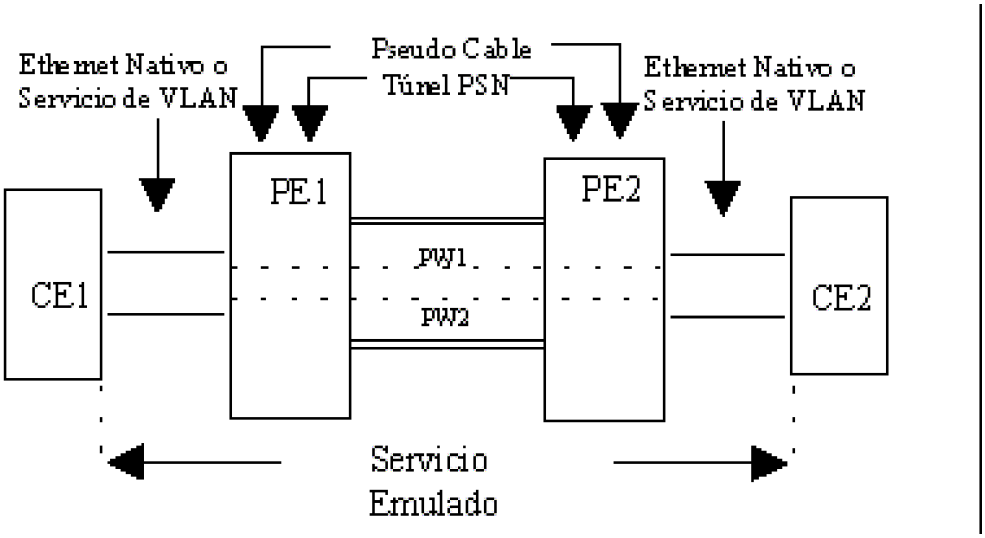

fig. 14

La figura 14 muestra un modelo de referencia para el esquema de pseudocable Ethernet.

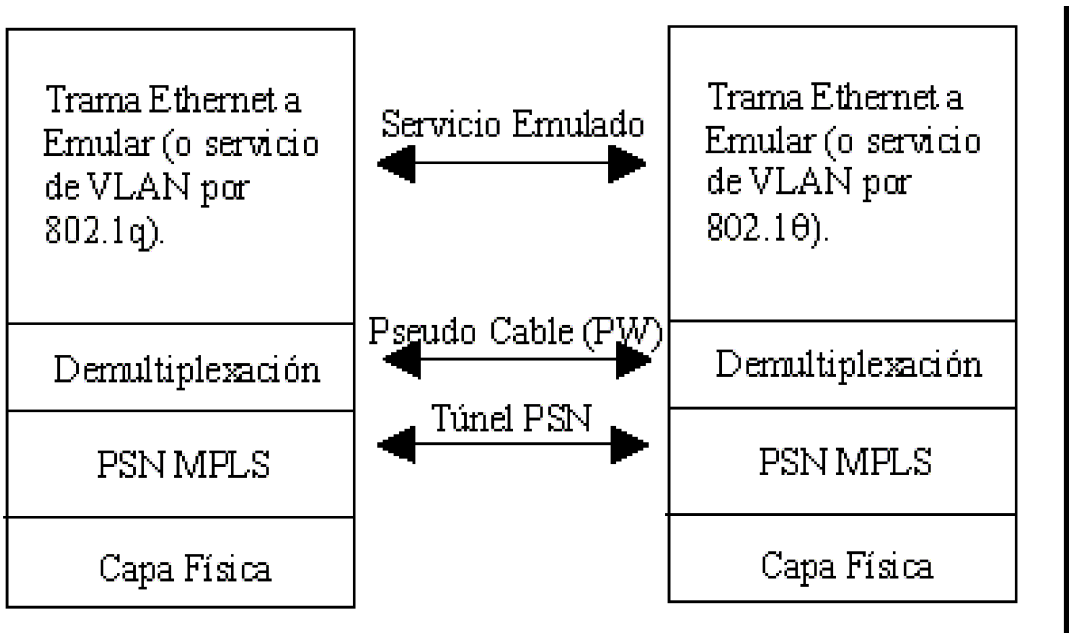

fig. 15

La figura 15 muestra el Stack de protocolos de Referencia para PWE (Pseudo Wired Ethernet).

Cuando un paquete se debe enviar desde PE1 a PE2 correspondiente a una trama ethernet de entrada, se realiza un push de una etiqueta MPLS para formar el túnel PSN (denominada "etiqueta PSN"). Ésta información no permite decirle al equipo PE2 qué hacer con el paquete que recibe (incluso con el uso de "penultimate hop popping"), por ello es necesaria otra etiqueta la cuál se denomina "etiqueta PW". En conclusión al igual que en el caso de BGP/MPLS VPNs se utiliza un stack de etiquetas de profundidad 2 [8]. La etiqueta PW no es visible hasta que el paquete llega al equipo PE2, toda la conmutación para el LSP se realiza a través de la etiqueta PSN. En la figura 15 se muestra el stack de protocolos que ilustra este punto.

La etiqueta PW puede interpretarse como la puerta Ethernet de salida o el identificador de VLAN de salida. El proceso es unidireccional y permite por ejemplo que dentro de una misma conexión, el identificador de VLAN en un extremo no coincida con el identificador en el otro.

En este caso debemos decir que quien tiene la tarea de realizar la sobre escritura de los identificadores de VLAN son los PE de entrada. Hay que destacar que un número ilimitado de etiquetas PWs pueden viajar a través de un sólo túnel PSN.

¿Cómo se distribuyen las etiquetas PW?, básicamente cualquier método usual, por ejemplo por asignación estática (configurándolas en los equipos PE1 y PE2) o por asignación dinámica, en éste último caso debe ser utilizando LDP en el modo "downstream unsolicited" y utilizando el mecanismo de descubrimiento extendido[9]. Se recomienda también la configuración de "liberal label retention".

Para poder interpretar la información que se distribuye por LDP se crea un nuevo tipo de FEC (128). Una única FEC se va a publicar por etiqueta PW. En la figura 16 se muestra el formato de los elementos intercambiados entre los LSR.

[8] "BGP/MPLS VPNs", E. Rosen, Y. Rekhter RFC 2547.
[9] "LDP Specification." L. Andersson, P. Doolan, N. Feldman, A.Fredette, B. Thomas. January 2001. RFC3036.

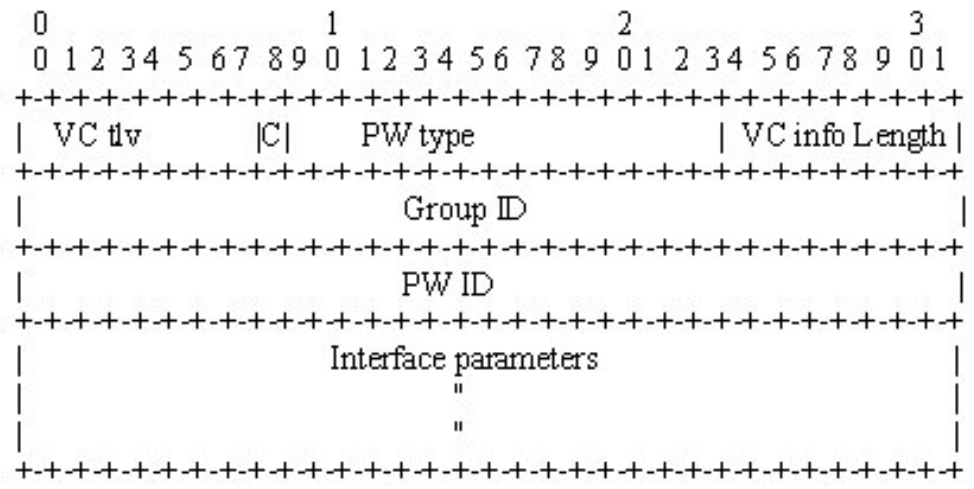

fig. 16

Donde se destacan los campos:

- PW Type: Tipo de VC, en especial Ethernet=0x0004, ATM=0x0003, FR=0x0001, etc.

- Group ID: Número de 32 bits que permite agrupar información de varios PW, permite por ejemplo enviar información de caída de puerto.

- PW ID: Número de 32 bits que junto al PW Type identifica a un PW.

- Interface Parameter Field: Aquí se definen distintos parámetros que incluyen MTU, Descripción de Interfaz e incluso solicitar al equipo de salida cuál es el número de VLAN Id deseado (si el equipo de ingreso no puede reescribirla).

Todos los números en estos campos son asignados por [10] y luego administrados por IANA.

[10] "Transport of Layer 2 Frames Over MPLS", Martini, L., et al., draft-ietf-pwe3-controlprotocol-01.txt, Noviembre 2002.

6.3 COMPARACIÓN DE VPLS CON L3-VPN.

La solución para ofrecer VPNs de nivel 3 utilizando MPLS está establecida en el RFC2347 [11], ésta consiste en implementar una solución de túneles a través de una pila de etiquetas de profundidad dos. La diferencia principal que se encuentra con respecto a la solución VPLS es que el plano de control viaja sobre BGP, utilizando los atributos RD correspondientes a las extensiones hechas sobre BGP. Cada PE que tiene algún cliente perteneciente a una VPN, establece conexiones BGP con el resto y conoce completamente la topología de la red a nivel de capa 3.

Por otro lado VPLS utiliza como protocolo LDP, donde se intercambian las etiquetas PW, a su vez los equipos PE no conocen la totalidad de la topología en lo que se refiere a tablas MAC, sino que se implementa como un gran switch trasparente.

Hay que destacar que las VPN de nivel 3 sobre MPLS fueron diseñadas de forma que poseen gran escalabilidad, siendo esto uno de sus mayores ventajas, mientras que las VPLS sólo se recomiendan para interconectar un número limitado de hosts.

6.4 COMPORTAMIENTO DE LOS FABRICANTES CON RESPECTO A LA TECNOLOGÍA VPLS.

En lo que se refiere a fabricantes de equipamiento, el mercado en éste sector ha estado extremadamente activo, en especial en aquellos que vienen del mundo IP, buscando desplazar a los grandes jugadores del mundo ATM.

Los fabricantes en general trabajan sobre la solución de dar implementaciones para comunicaciones punto a punto ethernet sobre MPLS. Existen opciones de implementaciones que no son compatibles con los denominados Martini-drafts, sino que toman como base los llamados Kompella-draft, por ende existe cierta discusión sobre cuál es la opción a tomar (dado que los primeros fueron los publicados por el grupo de trabajo pwe son la base para el presente trabajo). Algo interesante es que además de las implementaciones de fabricantes de

[11] "BGP/MPLS VPNs", E. Rosen, Y. Rekhter RFC 2547.

LSRs, ya existe una implementación sobre Unix, por ahora comercial. No hemos encontrado ninguna implementación de código abierto.

En lo que se refiere al mundo de los proveedores, en general todo aquel que cuenta con un backbone IP/MPLS, por ejemplo para dar servicios de VPNs de capa 3, simplemente realizando un cambio de software podrá dar servicios VPLS.

Podemos destacar a los siguientes fabricantes, quienes ya ofrecen en sus líneas de productos soluciones para conexiones punto a punto Ethernet sobre MPLS:

Cisco Systems

Juniper Network

Riverstone Networks

Nortel Networks

Alcatel Networks

IPInfusion (solución para equipos Unix).

6.5 VPLS JERÁRQUICO Y OPERACIONES MEJORADAS.

Con VPLS jerárquico (HVPLS), es posible crear una red jerárquica de dos o tres niveles. En la parte de acceso de la red se usa una clase nueva de conmutadores (switches) MPLS, también llamados conmutadores de unidad multiarrendatario (MTU), para agregar tráfico del cliente a los circuitos punto a punto Martini o Q-in-Q (Figura 13). Estos circuitos terminan dentro de los PEs VPLS. En lugar de crear una malla completa de MTUs, solo es necesario interconectar los PEs VPLS de "núcleo". Las MTUs están diseñadas de tal modo que sólo sea necesario un conjunto limitado de funciones MPLS para proporcionar dispositivos económicos y fáciles de administrar. Los Routers RS se pueden configurar por software para que funcionen como MTUs o PEs.

En la siguiente sección se describirá la manera en que también se pueden usar los circuitos entre dominios para romper la malla del núcleo entre dichos PEs de borde VPLS, a fin de proporcionar conectividad entre dominios y entre operadores. Las MTUs pueden tener conexiones múltiples a diferentes PEs VPLS para incrementar su confiabilidad.

Una vez creada una topología jerárquica, es posible optimizar aún más la replicación del tráfico, tanto de transmisión general (broadcast) como de multi-transmisión (multicast), para habilitar eficazmente aplicaciones como la distribución de video. El esfuerzo de la replicación se distribuye entre las MTUs de entrada o de salida, los PEs y los PEs de borde (Figura 17).

Sólo los sitios que escuchan flujos de multi-transmisión específicos reciben el tráfico correspondiente. Para ello, se usa el monitoreo (snooping) de IGMP y PIM para rastrear los puertos y los circuitos que pertenecen a un grupo de multi-transmisión específico, como se describe en[12] . También es posible minimizar el número de adyacencias de señalización LDP necesarias, ya que son menos los PEs que se interconectan entre sí. Esto también reduce el número total de LSPs requeridos entre los PEs desde $O(N^2)$ hasta $O(N)$.

La capacidad para ejecutar MPLS sobre enlaces agregados permite escalar los servicios VPLS de 1 Gbps a múltiples Gbps y ofrecer al mismo tiempo una mayor resistencia a fallas de enlaces.

Riverstone introdujo recientemente nuevas facilidades de OAM para detectar problemas de conectividad específicos de VPLS. Debido a que todavía no hay estándares disponibles para detectar fallas específicas de VPLS, Riverstone implementó estas nuevas facilidades con base en la retroalimentación de clientes.

[12] [VPLS-MCAST] draft-serbest-l2vpn-vpls-mcast (Internet Draft)

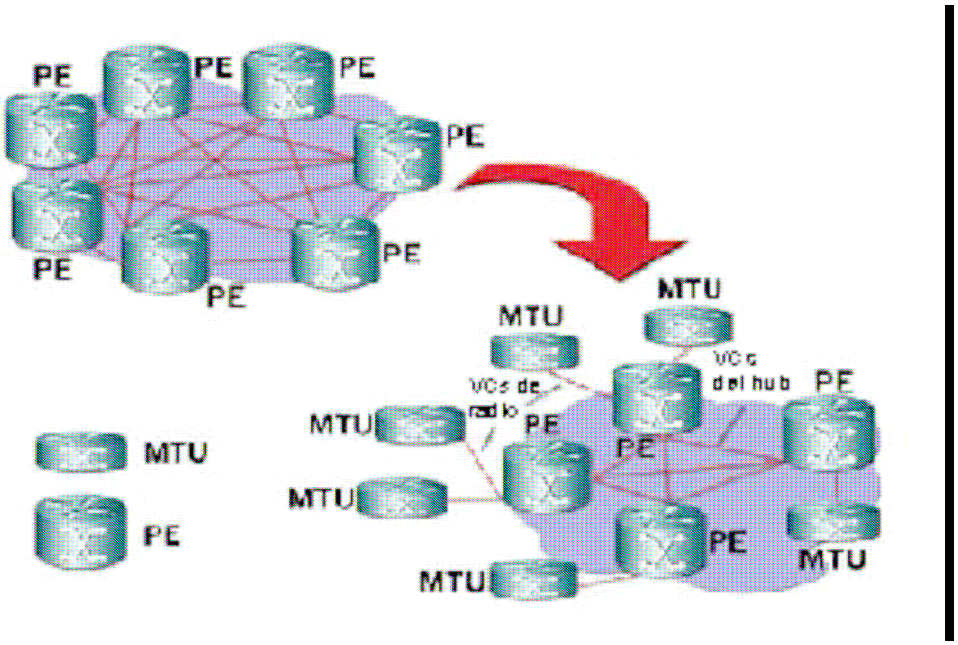

fig. 17

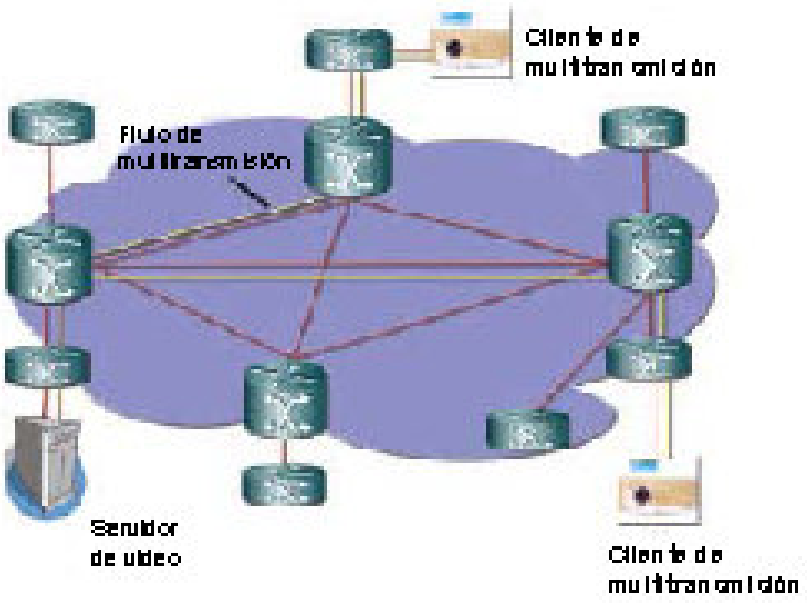

fig. 18

Tan pronto como los estándares estén disponibles, estas herramientas los cumplirán. Mientras que ping y traceroute de LSP se usan para detectar

problemas de transporte específicos de MPLS, ping y traceroute de VPLS se usan para detectar conectividad en el nivel MAC de Ethernet de todos los nodos conscientes de VPLS a lo largo del trayecto, tal como verificar que las direcciones MAC se hayan aprendido correctamente. Riverstone planea presentar un borrador IETF que describa estas extensiones de OAM.

En términos de alta disponibilidad, los routers RS y 15000 tienen redundancia en alimentación, matriz de conmutación y en el procesador principal. Riverstone también agregó capacidades Hitless Protection Switching (HPS) para hacer frente a las fallas de software.

Ante una falla o caída del procesador principal, el procesador de respaldo (que se mantiene sincronizado al principal) se hace cargo sin afectar los flujos del tráfico de datos manejados en el hardware. Esto incluye las capacidades de reinicio para la mayoría de los protocolos de enrutamiento y MPLS. Los routers de Riverstone separan las funciones de control y de transferencia. Los procesadores de control están dedicados a las funciones de control y administración, mientras que los ASICs y microprocesadores manejan las funciones de transferencia de datos. Esta distinción permite la transferencia de datos, incluso en el caso de fallas del software de control. Las capacidades de reinicio “amable” están disponibles para los protocolos de enrutamiento OSPF y BGP y también para los protocolos de señalización MPLS, como LDP y RSVP. Las extensiones de re-enrutamiento rápido RSVP-TE se pueden usar para establecer túneles LSP de respaldo para la reparación local de los túneles LSP. Se han especificado dos opciones de re-enrutamiento rápido: el método de respaldo uno a uno y el de respaldo de facilidades. Los routers de Riverstone usan la primera opción, la cual crea LSPs de desvío para cada LSP protegido en cada uno de los posibles puntos de reparación local.

Estas funciones permiten el uso de nuevas aplicaciones que requieren mayor disponibilidad y calidad para el servicio, como VoIP para que se ejecuten en las redes IP con MPLS habilitado y de agregación DSL sobre Ethernet, que usa VPLS como una tecnología de transporte de núcleo.

NIVELES DE OAM	
Herramientas de OAM	Nivel de detección de fallas
Ping y traceroute de VPLS	MAC
VCCV	VC LSP (PW)
Ping y traceroute de LSP	Túnel LSP
802.1ah y BFD	Enlace

*Nota: BFD también se puede usar junto con el ping de LSP y VCCV para mejorar la detección de fallas.

fig. 19

6.6 H-VPLS Inter-dominios / Inter-operadores.

La especificación actual de VPLS se extenderá para proveer conectividad entre dominios y entre operadores. La especificación de VPLS menciona que se pueden establecer enlaces Inter-dominio entre los PEs de borde (BPEs). Riverstone actualmente especifica la manera en que se pueden soportar y elegir de manera dinámica los BPEs redundantes, así como la forma en que se pueden usar conexiones Inter-dominios entre los BPEs para evitar puntos únicos de falla dentro de una red de núcleo (Figura 20).

También es posible usar el modelo de Operador de operadores VPN BGP para interconectar dominios VPLS, terminando los seudocables directamente en las instancias de ruteo y envío virtuales (VRF) RFC 2547 o correlacionando las VLANs 802.1q con las VRFs, como lo implementan actualmente algunos operadores.

Aunque Riverstone provee herramientas de aprovisionamiento de VPLS que automatizan la manera de configurar los servicios VPLS, la detección automática de PEs VPLS se puede lograr ya sea con BGP o con Radius. Aún está en debate cuál protocolo es el mejor para realizar la detección automática.

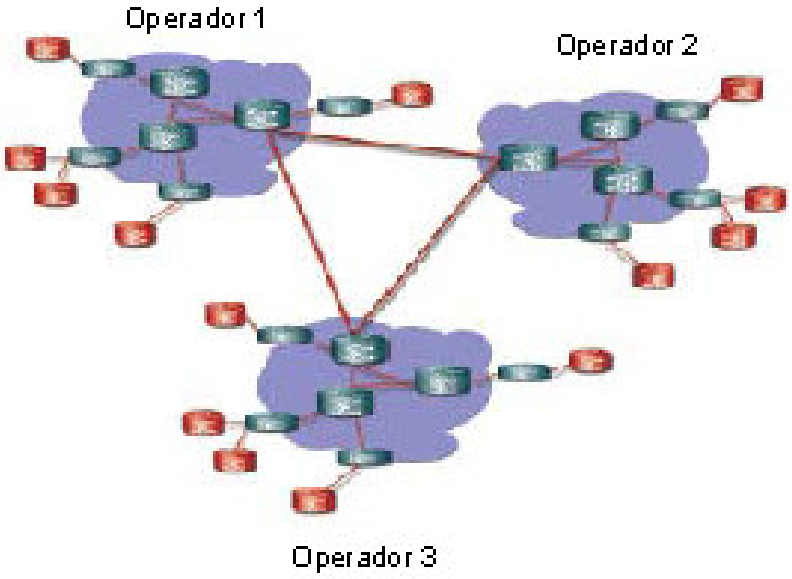

fig. 20

Ambos modelos son válidos y dependen de la construcción de la red SP. IETF ha desarrollado en realidad las dos propuestas como documentos para grupos de trabajo, lo que refleja el interés de la comunidad en ambas.

Existen muchas organizaciones de estándares que definen extensiones a las capacidades OAM de Ethernet y VPLS. Tanto IEEE 802.3ah como 802.1ag son de interés, así como las propuestas IETF BFD y VCCV.

Todos estos métodos diferentes son complementarios. Por ejemplo, 802.3ah es más adecuada para las verificaciones de conectividad de la última milla, mientras que BFD resulta más práctica para la comprobación de conectividad de enlaces dentro de las dorsales IP / MPLS del operador; VCCV permite la revisión individual de los seudocables dentro de los túneles MPLS.

El uso de LSPs punto a multipunto permitirá la adición de mejoras a las optimizaciones existentes de multi-transmisión (multicast) H-VPLS. Con HVPLS combinado con el monitoreo (snooping) de IGMP y PIN, los nodos conscientes de VPLS participan de manera inteligente en la tarea de replicación del tráfico de multi-transmisión, como se describe en las secciones anteriores. Con los LSPs punto multipunto, los nodos no conscientes de VPLS, como los routers P, también participan en la replicación del tráfico.

La interacción de Ethernet con ATM y Frame Relay, que se especifica en la Alianza ATM / FR de MPLS, también será mejorada, de tal forma que OAM y QoS se puedan suministrar de extremo a extremo. De este modo, los trayectos

de extremo a extremo se pueden tratar como conexiones lógicas, correlacionando tanto los perfiles de tráfico como el tráfico de OAM. Esto incluye la capacidad para vincular las fallas de PW con las notificaciones de falla de acceso al circuito y viceversa. Aunque el encapsulamiento en puente sobre ATM / FR no requiere una capa de adaptación específica para VPLS, el encapsulamiento ruteado requiere una función como la mediación ARP para correlacionar diferentes protocolos de resolución de direcciones entre tecnologías de acceso heterogéneas.

Con el tiempo, será mayor la necesidad de proveer una interacción dinámica entre dichas redes. Puesto que los routers de Riverstone tienen la capacidad para conectar ambas tecnologías, son adecuados para realizar las funciones de adaptación necesarias tales como:

Correlación de los protocolos de control ATM con los protocolos de control MPLS.

Señalización de PW's cuando hay solicitudes de señalización ATM UNI.

PWs dedicados para la señalización y ruteo ATM.

PWs como enlaces troncales virtuales para VPs ATM.

Funciones de mediación para PVCs de software.

La capacidad para interconectar (stitching) dos LSPs juntos, permitirá a los LSP cruzar los límites del operador o los dominios de TE. La TE entre áreas y entre AS brindará capacidades similares. La NNI (interfaz de red a red) de MPLS proporcionará herramientas para establecer acuerdos entre operadores que implican la conversión y correlación de diferentes niveles de calidad de servicio (QoS) y podrá proveer capacidades de ruteamiento entre diferentes operadores para cumplir con los SLAs requeridos.

En esta fase, se usará la opción de respaldo de la facilidad de re-enrutamiento rápido (fast-reroute). Se crearán túneles de desvío para proteger los posibles puntos de falla. Dichos túneles pueden proteger a un grupo de LSPs protegidos con restricciones de respaldo semejantes.

Finalmente, con MPLS en la línea divisoria entre la conmutación (plano de datos) y el ruteo (plano de control), Riverstone planea proporcionar capacidades uniformes de L2 y L3 en su línea de productos:

• Un componente importante en QoS es la capacidad de ver la información del encabezado de L3, como las marcas DSCP, durante la toma de decisiones de transferencia en L2.

En lugar de depender de las prioridades de 802.1p, que no siempre pueden estar disponibles o ser confiables, los PEs VPLS pueden examinar los códigos de punto ToS / DSCP y la combinación del puerto entrante / VLAN para determinar el mejor trayecto hacia un destino y marcar los bits EXP de MPLS según corresponda.

• La capacidad para terminar los dominios de L2 dentro de los dominios de L3 dentro de la misma plataforma elimina la necesidad de usar una solución de dos cajas para proveer acceso a Internet, por ejemplo. Esto significa que los PWs Martini y VPLS necesitan terminarse y correlacionarse con una interfaz de ruteo IP (o una VRF). Por lo tanto, los PWs se usan como puertos virtuales y por ello se pueden usar como cualquier otro puerto físico o lógico. Una combinación de circuitos virtuales Ethernet, ATM / FR y de PWs de MPLS pueden ser parte del mismo dominio de L2 con una interfaz ruteada para Internet, por ejemplo

• La capacidad para que IP maneje un gran número de direcciones MAC, la cual requiere una gran tabla de IP-ARP o capacidades de monitoreo (snooping) DHCP.

• La capacidad para equilibrar el espacio usado para las rutas IP con las direcciones MAC permite que la memoria especializada y de alto rendimiento como la memoria de contenido direccionable (CAM) se comparta de manera eficiente, dependiendo del tipo de servicio que se ofrezca sobre una plataforma[13].

6.7 EJEMPLO DE CONFIGURACIÓN DE VPLS SOBRE ROUTERS CISCO.

Aprovechando la existencia ya de implementaciones de diferentes fabricantes, tomaremos una para verificar el comportamiento de la solución propuesta respecto a la teoría presentada en este trabajo. Los equipos utilizados serán del fabricante Cisco Systems.

[13] www.riverstonenet.com/spanish/ pdf/mpls_vpls_evolution_spanish.pdf

La prueba será únicamente de verificación del comportamiento de los equipos respecto al servicio VPLS, no se tomarán consideraciones de seguridad ni de desempeño o escala.

En la figura 21 podemos ver el esquema de pruebas, el cuál consiste en dos equipos PE conectados a través de MPLS, con LDP configurado entre ellos y dos trunks 802.1q hacia dos clientes.

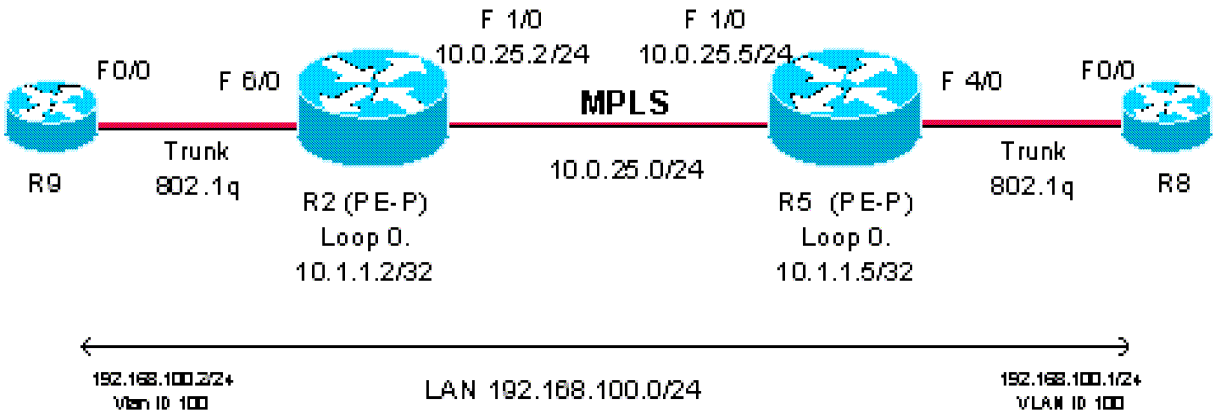

fig. 21

Debemos destacar lo siguiente:

· Los equipos R2 y R5 (modelo Cisco 7206 con tarjetas Fast Ethernet), cumplen funciones de P y PE de la nube MPLS. Entre ellos corre el protocolo interno de enrutamiento OSPF, de forma que ambos equipos son vecinos del mismo. También se establece entre ellos (a través de las loopbacks) una sesión LDP por donde transita el tráfico de señalización MPLS. En las interfaces hacia los clientes (CE) estos equipos no tienen configurada dirección IP.

Los equipos R8 y R9 cumplen la función de clientes (CE) y ellos sólo tienen configurada una dirección IP correspondiente a la red 192.168.100.0/24.

Debemos destacar que el fabricante Cisco Systems sólo acepta que la conexión CE-PE sea a través de un trunk 802.1q, aunque se utilice una sola VLAN.

Las pruebas realizadas cubrieron los puntos de comunicación básica (a través del protocolo ICMP), relevamiento de las sesiones OSPF y LDP, estudio de las tablas de etiquetas y análisis del intercambio de datos y señalización entre ambos PEs.

Tomaremos como base a los equipos R2 y R9.

A continuación se muestra la configuración de la interfaz entre ambos equipos:

R2:

```
!
interface FastEthernet6/0
no ip address
duplex full
tag-switching ip
!
interface FastEthernet6/0.100
encapsulation dot1Q 100
mpls l2transport route 10.1.1.5 100
!
```

Donde el último número (100) del comando mpls l2transport es el identificador PWID (al cuál Cisco llama VC) para esta conexión entre R2 y R5 (pueden haber más de uno). La dirección IP del mismo comando corresponde al PE de salida (R5).

R9:

```
!
interface FastEthernet0/0
no ip address
no ip directed-broadcast
no keepalive
speed 100
full-duplex
!
interface FastEthernet0/0.100
encapsulation dot1Q 100
ip address 192.168.100.2 255.255.255.0
no ip directed-broadcast
```

La primera prueba consiste en verificar la existencia de conectividad IP entre R9 y R8:

r9#ping 192.168.100.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.100.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

r9#sh arp

Protocol Address Age (min) Hardware Addr Type Interface

Internet 192.168.100.1 5 0004.4ea5.0038 ARPA FastEthernet0/0.100

Internet 192.168.100.2 - 0030.190a.c9a0 ARPA FastEthernet0/0.100

r9#

Donde la dirección MAC que se observa en R9 corresponde a la interfaz de R8 y no a la de R2, por lo que se verifica que los paquetes ARP viajan en forma trasparente hasta el otro extremo y no se trata de ninguna configuración del tipo proxy-arp.

Respecto a R2, vemos la sesión LDP con R5 levantada:

r2#sh mpls ldp neighbor

Peer LDP Ident: 10.1.1.5:0; Local LDP Ident 10.1.1.2:0

TCP connection: 10.1.1.5.11013 - 10.1.1.2.646

State: Oper; Msgs sent/rcvd: 12/12; Downstream

Up time: 00:05:04

LDP discovery sources:

FastEthernet1/0, Src IP addr: 10.0.25.5

Targeted Hello 10.1.1.2 -> 10.1.1.5, active, passive

Addresses bound to peer LDP Ident:

10.0.25.5 10.1.1.5

r2#

La tabla de rutas nos da la información a nivel de Capa 3 (convergencia OSPF):

r2#sh ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

** - candidate default, U - per-user static route, o - ODR*

P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks

C 10.1.1.2/32 is directly connected, Loopback0

O 10.1.1.5/32 [110/2] via 10.0.25.5, 00:01:10, FastEthernet1/0

C 10.0.25.0/24 is directly connected, FastEthernet1/0

También observamos los comandos propios del transporte ethernet:

r2#sh mpls l2transport summary

Destination address: 10.1.1.5, total number of vc: 1

0 unknown, 1 up, 0 down, 0 admin down

1 active vc on MPLS interface Fa1/0

r2#

r2#sh mpls l2transport binding 100

Destination Address: 10.1.1.5, VC ID: 100

Local Label: 16

Cbit: 1, VC Type: Ethernet, GroupID: 5

MTU: 1500, Interface Desc: n/a

Remote Label: 16

Cbit: 1, VC Type: Ethernet, GroupID: 3

MTU: 1500, Interface Desc: n/a

r2#

Donde ya tenemos la información no sólo del PWID sino también de la Label a utilizar para ésta.

La información más detallada se observa en el siguiente comando:

r2#sh mpls l2transport vc 100 detail

Local interface: Fa6/0.100 up, line protocol up, Eth VLAN 100 up

Destination address: 10.1.1.5, VC ID: 100, VC status: up

Tunnel label: imp-null, next hop 10.0.25.5

Output interface: Fa1/0, imposed label stack {16}

Create time: 00:08:29, last status change time: 00:07:29

Signaling protocol: LDP, peer 10.1.1.5:0 up

MPLS VC labels: local 16, remote 16

Group ID: local 5, remote 3

MTU: local 1500, remote 1500

Remote interface description:

Sequencing: receive disabled, send disabled

VC statistics:

packet totals: receive 19, send 11

byte totals: receive 3894, send 1278

packet drops: receive 0, send 0

Debido a la arquitectura de la prueba propuesta, se puede percibir el problema que ocurre en MPLS con las tramas ethernet de tamaño cercano a los 1500bytes. Sabemos que en una LAN ethernet la MTU por defecto es 1500 bytes, si a tramas de éste tamaño se le agrega el encabezado MPLS, obtenemos los llamadas "jumbo frames". En el siguiente comando vemos que tramas de 1490 bytes no logran atravesar la nube MPLS.

r8#ping

Protocol [ip]:

Target IP address: ping192.168.100.2

Repeat count [5]:

Datagram size [100]: 1490

Timeout in seconds [2]:

Extended commands [n]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 1490-byte ICMP Echos to 192.168.100.2, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

r8#

Dado que el problema ocurre debido a que se utilizaron interfaces FastEthernet en el núcleo de la red, la solución consiste en aumentar el MTU en éstas interfaces a 1512 bytes. Si existieran switches también es necesario aumentarles el MTU [14].

[14] VPLS – MPLS Ing Roque Gagliano IIE-Facultad de Ingeniería 2002-2003

7. CONCLUSIONES.

La tecnología de conmutación en Backbones de operador ha evolucionado rápidamente para beneficio de los proveedores del servicio de Internet y para beneficio de los usuarios que requieren cada día más y mejores tecnologías de comunicación, las tecnologías que actualmente están ingresando al mercado con fuerza como (MPLS/VPLS), son menos complejas y más transparentes para el usuario, además permiten la utilización de las infrestructuras existentes.

MPLS no se desarrollo para cambiar la tecnología de enrutamiento actual, ni para ser un protocolo que se utilice a nivel WAN, tampoco fue desarrollado para optimizar el ancho de banda; las verdaderas razones de su creación son: funcionar sobre cualquier tecnología de transporte no sólo ATM, soportar el envío de paquetes tanto unicast como multicast, permitir el crecimiento constante de la Internet y además ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP.

MPLS no fue un protocolo creado para sustituir los protocolos de enrutamiento existentes, en Internet siempre será un requisito el enrutamiento de capa 3 por los siguientes motivos: por la imposibilidad de hacer filtrado de paquetes (firewalls), por la poca probabilidad que hay de implantar soluciones MPLS en los sistemas finales y porque las etiquetas solo pueden tener un significado local.

La diferencia con topologías conectivas reales es que en MPLS la construcción de caminos virtuales es mucho más flexible y que no se pierde la visibilidad sobre los paquetes IP. Todo ello abre enormes posibilidades a la hora de mejorar el rendimiento de las redes y de soportar nuevas aplicaciones de usuario.

Las ventajas de VPLS son muchas, el solo hecho de permitir que los equipos de una red corporativa ubicados en distintos puntos en una área metropolitana puedan ver de forma transparente un Backbone metropolitano como un gran switch único es una ventaja fundamental, especialmente para aquellas empresas que tienen redes dispersas a nivel metropolitano y presentan una gran demanda de ancho de banda.

Enfocando las conclusiones hacia el verdadero propósito de esta monografía, que es mostrar a VPLS como una tecnología atractiva para los operadores de servicio y para las empresas que requieren de servicios de comunicación óptimos entre sus sucursales; podemos concluir que los servicios que esta tecnología presta como lo son: escalabilidad, multitransmisión (multicast) mejorada, alta disponibilidad, localización de fallas de extremo a extremo, prestación rápida de servicios en zonas geográficas amplias con QoS entre operadores, facilidad de aprovisionamiento y localización de fallas, son razones suficientes para determinar que MPLS/VPLS se va a convertir en la tecnología estándar a utilizar en los Backbones metropolitanos de los operadores de servicios.

Es importante también aclarar que MPLS/VPLS también trae consigo ciertas limitaciones directamente ligadas al número de VLANS y PEs dentro de un Backbone, pero que aún así es una tecnología importante que trae muchos beneficios.

Por ultimo y después de analizar el ejemplo de implementación expuesto dentro del trabajo, podemos destacar dos aspectos importantes que se pudieron visualizar; primero la dirección MAC que se observa en R9 corresponde a la interfaz de R8 y no a la de R2, por lo que se verifica que los paquetes ARP viajan en forma transparente hasta el otro extremo y no se trata de ninguna configuración del tipo proxy-arp, y segundo podemos percibir el problema que se presentan con las llamadas ‘’Jumbo Frames’’ que no logran atravesar la nube MPLS.

RECOMENDACIONES

La presente investigación utiliza el enfoque expuesto por la empresa Riverstone en sus artículos sobre MPLS/VPLS, este enfoque reconoce 4 etapas evolutivas, la primera etapa habla de los antecedentes y de MPLS como la nueva tecnología en los Backbones Metropolitanos, la segunda etapa habla de VPLS y Seudocables Martini, la tercera etapa habla de H-VPLS y por ultimo se habla de H-VPLS interdominios interoperadores; este enfoque permite al lector del presente trabajo comprender todos los conceptos de una forma coherente y consecuente; para los lectores que tienen alguna experiencia en los conceptos preliminares de esta investigación pueden enfocarse solo en los capítulos de MPLS y VPLS. Siempre que se hable de VPLS es importante hacer un repaso de la teoría de MPLS, Finalmente para el lector será importante poder analizar y abstraer las ventajas que dichas tecnologías traen consigo y también sería interesante analizar el ejemplo de configuración de VPLS propuesto en la investigación y sacar sus propias conclusiones sobre este.

Seria importante ampliar algunos conceptos que no fueron tratados tan profundamente en esta investigación, entre ellos probar las facilidades de OAM que presenta VPLS y además montar una maqueta de pruebas más amplia sobre la cual se puedan evaluar todas las facilidades que trae consigo la implementación de VPLS sobre un Backbone metropolitano.

BIBLIOGRAFIA

[LDP] LDP specification (RFC3036), LDP State Machine (RFC3215).

[MPLS-ARCH] MPLS Architecture (RFC3031), MPLS Label Snack Encoding (RFC3032).

[RSVP-TE] RSVP-TE extensions for LSP tunnels (RFC3209).

[VPLS-APPLIC] draft-ietf-l2vpn-vpls-ldp-applic (Internet Draft).

[VPLS-LDP] draft-ietf-l2vpn-vpls-ldp (Internet Draft).

[VPLS-MCAST] draft-serbest-l2vpn-vpls-mcast (Internet Draft).

"BGP/MPLS VPNs", E. Rosen, Y. Rekhter RFC 2547.

"Transport of Layer 2 Frames Over MPLS", Martini, L., et al., draft-ietf-pwe3-controlprotocol-01.txt, Noviembre 2002.

"LDP Specification." L. Andersson, P. Doolan, N. Feldman, A.Fredette, B. Thomas. Enero 2001. RFC3036

"Encapsulation Methods for Transport of Ethernet Frames Over IP/MPLS Networks" Martini, L., et al., draft-ietf-pwe3-ethernet-encap-01.txt, Noviembre 2002.

MPLS "Multiprotocol Label Switching": Una arquitectura de Backbone para la Internet del Siglo XXI. María Sol Canalis. Departamento de Informática. Universidad Nacional del Nordeste. Corrientes. Argentina. En Internet: www.red-mpls.udg.es/presentaciones/rpv_mpls.pdf

Artículos técnicos de Riverstone Network, Evolución de MPLS/VPLS una perspectiva de Riverstone en Internet: www.riverstonenet.com/spanish/ pdf/mpls_vpls_evolution_spanish.pdf

www.overturenetworks.com/ pdfs/products/ISG5000_DATA_SPANREV1.pdf

CISCO IOS MPLS VIRTUAL PRIVATE LAN SERVICE Business Overview Enabling Innovative Services en Internet: www.cisco.com/application /pdf/en/us/uest/tech/tk891/c1482/ccmigration_09186a00801ed3ea.pdf

CISCO IOS MPLS VIRTUAL PRIVATE LAN SERVICE en Internet : www.cisco. com/en/US/about/ac123/ac114/ac173/Q2-4/technology_a_case_for _VPLS.html - 32k.

NORMA 802.1q en Internet: standards.ieee.org/getieee802/download/802.1Q-2003.pdf

ANEXO A.

CARACTERÍSTICAS DE LOS EQUIPOS UTILIZADOS EN LA PRUEBA EXPUESTA DENTRO DE LA MONOGRAFÍA Y SUS CONFIGURACIONES

R2 y R5:
Cisco 7206VXR
128M DRAM
20M Flash Card

Tarjetas:
PA-2FEISL
PA-FE-TX
IOS: c7200-p-mz.122-14.S.bin

R8 y R9:
Cisco 2621
48M DRAM
16M Flash
IOS: c2600-is-mz.120-7.T.bin
Configuraciones:

R2:

```
r2#sh run
Building configuration...
Current configuration : 1238 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname r2
!
logging snmp-authfail
!
ip subnet-zero
ip cef
!
!
!
mpls label protocol ldp
mpls ldp logging neighbor-changes
tag-switching tdp router-id Loopback0 force
call rsvp-sync
!
!
!
controller E1 3/0
!
controller E1 3/1
!
controller E1 3/2
!
controller E1 3/3
```

```
!
controller E1 3/4
!
controller E1 3/5
!
controller E1 3/6
!
controller E1 3/7
!
interface Loopback0
ip address 10.1.1.2 255.255.255.255
!
interface FastEthernet1/0
description Conexión con R5
ip address 10.0.25.2 255.255.255.0
duplex full
mpls label protocol ldp
tag-switching ip
!
interface FastEthernet1/1
no ip address
duplex half
!
interface ATM4/0
no ip address
shutdown
!
interface ATM5/0
no ip address
shutdown
!
interface FastEthernet6/0
description Conexión con R9
no ip address
duplex full
tag-switching ip
!
interface FastEthernet6/0.100
description VLAN a transportar
encapsulation dot1Q 100
mpls l2transport route 10.1.1.5 100
!
router ospf 100
log-adjacency-changes
network 10.0.25.0 0.0.0.255 area 0.0.0.0
network 10.1.1.0 0.0.0.255 area 0.0.0.0
!
ip classless
no ip http server
!
dial-peer cor custom
!
line con 0
stopbits 1
line aux 0
```

stopbits 1
line vty 0 4
login
!
end

R5:
r5#sh run
Building configuration...
Current configuration : 1181 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname r5
!
logging snmp-authfail
!
ip subnet-zero
ip cef
!
!
mpls label protocol ldp
mpls ldp logging neighbor-changes
tag-switching tdp router-id Loopback0 force
call rsvp-sync
!
!
controller E1 3/0
!
controller E1 3/1
!
controller E1 3/2
!
controller E1 3/3
!
controller E1 3/4
!
controller E1 3/5
!
controller E1 3/6
!
controller E1 3/7
!
!
!
interface Loopback0
ip address 10.1.1.5 255.255.255.255
!
interface FastEthernet1/0
ip address 10.0.25.5 255.255.255.0
duplex full
mpls label protocol ldp

tag-switching ip
!
interface FastEthernet1/1
no ip address
duplex full
tag-switching ip
!
interface FastEthernet4/0
no ip address
duplex full
!
interface ATM6/0
no ip address
shutdown
!
router ospf 100
log-adjacency-changes
network 10.0.25.0 0.0.0.255 area 0.0.0.0
network 10.1.1.0 0.0.0.255 area 0.0.0.0
!
ip classless
no ip http server
!
!
dial-peer cor custom
!
!
line con 0
exec-timeout 0 0
logging synchronous
stopbits 1
line aux 0
stopbits 1
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
!
end

R9:
r9#sh run
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname r9
!
!
ip subnet-zero

no ip domain-lookup
!
!
interface FastEthernet0/0
no ip address
no ip directed-broadcast
no keepalive
speed 100
full-duplex
!
interface FastEthernet0/0.100
encapsulation dot1Q 100
ip address 192.168.1.2 255.255.255.0
no ip directed-broadcast
!
interface Serial0/0
no ip address
no ip directed-broadcast
no ip mroute-cache
shutdown
no fair-queue
!
interface FastEthernet0/1
no ip directed-broadcast
no keepalive
shutdown
speed 100
full-duplex
!
interface Serial0/1
no ip address
no ip directed-broadcast
shutdown
!
!
ip classless
no ip http server
!
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end

R8:
r8#sh run
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption

```
!
hostname r8
!
!
ip subnet-zero
no ip domain-lookup
!
!
interface FastEthernet0/0
no ip address
no ip directed-broadcast
no keepalive
speed 100
full-duplex
!
interface FastEthernet0/0.100
encapsulation dot1Q 100
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast
!
interface Serial0/0
no ip address
no ip directed-broadcast
no ip mroute-cache
shutdown
no fair-queue
!
interface FastEthernet0/1
no ip directed-broadcast
no keepalive
shutdown
speed 100
full-duplex
!
interface Serial0/1
no ip address
no ip directed-broadcast
shutdown
!
!
ip classless
no ip http server
!
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

ANEXO B.

Data Sheet

Cisco 7200 Series Router

The Cisco 7200 Series Router delivers exceptional performance/price, modularity, and scalability in a compact form factor with a wide range of deployment options. With processing speeds up to 1 million packets per second, port adapters ranging from NxDS0 to OC-12, and an unparalleled number of high-touch IP services, the Cisco 7200 is the ideal WAN edge device for enterprises and service providers deploying any of the following solutions:

• *WAN edge*—Award-winning quality-of-service (QoS) features performance.

• *Broadband aggregation*—Up to 8,000 Point-to-Point Protocol (PPP) sessions per chassis.

• *Multiprotocol Label Switching provider edge (MPLS PE)*—Number one choice for
provider edge deployment today.

• *Voice/video/data integration*— Time-division multiplexer (TDM)-enabled VXR chassis and voice port adapters.

• *IP Security virtual private networking (IPSec VPN)*—Scalable to 5,000 tunnels per chassis.

• High-end customer premises equipment (CPE).

• The Cisco 7200 addresses these solution requirements by integrating functions previously performed by separate devices into a single platform. Through this integration, the Cisco 7200 provides a single, cost-effective platform that supports:

• High-density LAN and WAN interfaces.

• Broadband subscriber services aggregation, including PPP, RFC 1483 termination, and Layer 2 Tunneling Protocol (L2TP) tunneling.

• Digital T1/E1 TDM trunk termination for voice, video, and data.

• High-density multichannel T3/E3 and T1/E1 with integrated channel service unit/data service unit (CSU/DSU).
• ATM, Packet over SONET (POS), and Dynamic Packet Transport (DPT) connectivity.

• Direct ATM Circuit Emulation Standard (CES) connectivity for voice, video, and data.

• Direct IBM mainframe channel connectivity.

• Light-density Layer 2 Ethernet switching.

Figure 1
The Cisco 7200 Router Series.

The Cisco 7200 Series offers a rich set of capabilities that address requirements for performance, density, high reliability, availability, serviceability, and anageability (Table 1).

Table 1 Cisco 7200 Features and Benefit.

Features	Benefits
Up to 1 Mpps processing capability	Provides high-performance routing and processing performance
Maximum connectivity options	Meets a variety of topology requirements with the widest range of port densities and interface options
Breadth of services	Supports QoS, security, MPLS, broadband, multiservice, and management features for next-generation networks
Investment protection	Low initial investment with upgrade and redeployment capability

Applications

• *VPN gateways*—With the new VPN Acceleration Module (VAM), the Cisco 7200 provides high-performance, hardware-assisted encryption, key generation, and
compression services suitable for site-to-site VPN applications.

• *Broadband subscriber aggregation services*—For small- and medium-density aggregation for network operators, competitive local exchange carriers (CLECs), Internet service providers (ISPs), post, telephone, and telegraph

networks (PTTs), and enterprises worldwide, the Cisco 7200 offers differentiated, value-added service platform with hardware-accelerated Parallel Express Forwarding (PXF) services. Key features include:

- Flexible, modular interfaces for traffic aggregation: OC-3, DS3, Fast Ethernet, Gigabit Ethernet, POS.
- IP and ATM QoS/class of service (CoS).
- MPLS VPN and full L2TP support.
- Feature-rich IP services and PPP termination support.

• *Multiservice capabilities*—The Cisco 7200 Series provides a scalable voice gateway solution, ranging from 2 to 20 T1s and E1s. The advanced QoS and multiservice features of the Cisco 7200 Series makes it an ideal platform in a large number of enterprise and service provider deployments as managed multiservice CPE or as a voice gateway.

• *Managed network services CPE*—The Cisco 7200 is a cost-effective CPE solution with a field upgradable modular platform. Key features for revenue-generating services include QoS, MPLS (MPLS VPN, MPLS QoS, MPLS TE), WAN edge services (VLAN support, NetFlow, NBAR), Security services (NAT, ACL, hardware encryption for VPNs), and voice/video/data integration.

• *Enterprise WAN aggregation*—The Cisco 7200 provides a flexible aggregation solution that accommodates a wide range of connectivity and service options, offers high quality and reliability, and can scale to meet future requirements. The Cisco 7200's performance per price ratio in the DS0 to OC-3/STM1 range makes it the ideal platform for aggregating multiple branch offices or remote locations.

Product Specifications

Cards, Ports, Slots

Table 2

	Cisco 7204VXR	Cisco 7206VXR
Configurable Slots	4	6
Ethernet (10BASE-T) Ports	32	48
Ethernet (10BASE-FL) Ports	20	30
Fast Ethernet (TX) Ports	4	Up to 6
Fast Ethernet (FX) Ports	4	Up to 6
EtherSwitch Port Adapters	2	2
100VG-AnyLAN Ports	4	Up to 6
FDDI (FDX, HDX) Ports	0	0
ATM Ports (T3, OC-3)	4, 4	Up to 6, 4
Packet over SONET	2	2
ATM-CES Port Adapters (Data, Voice, Video), Dual-Wide	1	1
Token Ring (FDX, HDX) Ports	16	24
Synchronous Serial Ports	32	48
ISDN BRI Ports (U, S/T)	16, 32	24, 48
ISDN PRI, Multichannel T1/E1 Ports	32	48
Multichannel T3 Ports	Up to 4	Up to 6
HSSI Ports	Up to 8	Up to 12
Packet over T3/E3 Ports (Integrated DSU)	Up to 8	Up to 12
IBM Channel Interface Ports (ESCON and Parallel)	6	6
VPN Acceleration Module	1	1

Chassis

Tabla 3.

Feature	Cisco 7204VXR	Cisco 7206VXR
Chassis/Rack	16 with side-to-side air flow 9 with RDS mounting system for front-to-back airflow	Same as Cisco 7204VXR
I/O Card slots	1	Same as Cisco 7204VXR
Port Adapter Slots	4	6
Midplane	2 independent 32-bit, 50-MHz PCI buses with an aggregate bandwidth of 1.6 Gbps when used with NPE-400 or above	Same as Cisco 7204VXR

Feature	Cisco 7204VXR	Cisco 7206VXR
Online Insertion and Removal (OIR)	Yes	Same as Cisco 7204VXR
Field-Replaceable Components	Processor, memory, power supply, I/O card, and port adapters	Same as Cisco 7204VXR
Additional Standard Components	AC power supply, AC power cord	Same as Cisco 7204VXR

• The Cisco 7200 Series VXR chassis also include a Multiservice Interchange (MIX), which supports switching of DS0 time slots via MIX interconnects across the midplane to each port adapter slot.

• The midplane and the MIX also support distribution of clocking between channelized interfaces on the Cisco 7200 to support voice and other constant-bit-rate applications. The VXR midplane provides two full-duplex 8.192-Mbps TDM streams between each port adapter slot and the MIX, which is capable of switching DS0s on all 12 8.192-Mbps streams. Each stream can support up to 128 DS0 channels.

• The MIX in the Cisco 7200VXR provides the ability to switch DS0 time slots between multichannel T1 and E1 interfaces, much like TDM capabilities. This enables the Cisco 7200VXR to switch DS0 voice channels on a T1/E1 interface on one port adapter to and from separate voice-processing port adapters. It also enables DS0s to be switched through the Cisco 7200VXR without any processing, which is a requirement in certain voice configurations.

Processors

• The Cisco 7200 Series sets new standards in meeting requirements for high-performance Layer 3 services at an affordable price for both service providers and enterprises.

• The following processors are currently available for the Cisco 7200 Series:
  – NPE-225
  – NPE-400
  – NSE-1
  – NPE-G1

• The NPE processors offer exceptional price/performance for most applications, including enterprise WAN aggregation, CPE, multiservice, and VPN. These processors provide the greatest flexibility when deploying new features.

• The NSE-1 Network Services Engine takes advantage of PXF to offer services acceleration for “high-touch” edge services for applications such as broadband and leased-line aggregation.

• Key features supported by the Cisco 7200 Series processors include security, QoS, traffic management, and network management.
• More information on the Cisco 7200 processors is available at:

http://www.cisco.com/warp/public/cc/pd/rt/7200/prodlit/npe72_ds.htm
http://www.cisco.com/warp/public/cc/pd/ifaa/prossor/nse1/
http://www.cisco.com/warp/public/cc/pd/ifaa/prossor/prodlit/npeg1_ds.htm

Input/Output Controllers

• Each Cisco 7200 Series chassis has a dedicated slot for an I/O controller. The following types of I/O controllers are currently supported, including some with LAN ports for increased density without using a port adapter slot:

– C7200-I/O, Cisco 7200 I/O Controller.

– C7200-I/O-2FE/E, Cisco 7200 I/O Controller with dual autosensing 10/100 Ethernet ports.

– C7200-I/O-GE+E, Cisco 7200 I/O Controller with 1 Gigabit Ethernet Interface Converter (GBIC) port and one Ethernet port.

Environmental Conditions

Table 4

	Cisco 7204VXR	Cisco 7206VXR
Operating temperature	32 to 104 F (0 to 40 C)	Same as Cisco 7204VXR
Storage temperature	-4 to 149 F (-20 to 65 C)	Same as Cisco 7204VXR
Operating humidity	10 to 90% (noncondensing)	Same as Cisco 7204VXR

Interfaces

• The Cisco 7200 Series offers scalable density with the widest range of connectivity options including:
– Ethernet 10BASE-T and 10BASE-FL
– Fast Ethernet 100BASE-T (RJ-45 and MII)
– Gigabit Ethernet
– Token Ring (half and full duplex)
– Synchronous serial ISDN BRI, PRI, HSSI, T3, E3
– Multichannel T1, ISDN PRI
– Multichannel E1, ISDN PRI
– Multichannel T3, E3
– Multichannel STM-1
– Packet Over SONET (POS)
– Dynamic Packet Transport (DPT)
– ATM (single-mode and multimode)
– ATM-CES
– Digital Voice Port Adapter, Enhanced
– Mix-enabled T1/E1
– Integrated Service Adapter (ISA)
– VPN Acceleration Module (VAM)

• The Cisco 7200 shares the same port adapters with the Cisco 7400, 7500, and 7600 FlexWAN module, protecting customer investment in interfaces, providing a clear migration path, and simplifying sparing.

• More detailed information on specific port adapters is available at:

http://www.cisco.com/warp/public/cc/pd/ifaa/pa/index.shtml

Options—Features

Key features supported by the Cisco 7200 include:

• Cisco Express Forwarding
• QoS
– Low-Latency Queuing (LLQ)
– Class-Based Weighted Fair Queuing (CBWFQ)
– Class-Based Weighted Random Early Detection (CBWRED)
– Policing
– Marking
– Shaping
– Committed Access Rate (CAR)
– Generic Traffic Shaping (GTS)
– Frame Relay Traffic Shaping (FRTS)
– Modular QoS command-line interface (MQC) support
• MPLS
– MPLS VPN
– MPLS QoS
– MPLS traffic engineering
• Broadband aggregation
– PPPoX
– RBE
– PPP over X (PPPoX) with L2TP
– MLPPP
• Multiservice/voice
– cRTP
– LFI
– FRF11/12
– MLPPP
– MLFR
• Tunneling
– GRE
– L2TP
– UTI
• Other
– ACLs
– NAT
– NetFlow
– Firewall
– Multicast

Performance

• Up to 225 kpps with NPE-225 processor
• Up to 400 kpps with NPE-400 processor

• Up to 300 kpps with accelerated services with NSE-1 processor
• Up to 1 Mpps with NPE-G1 processor

Memory

Table 5

	Cisco 7204VXR	Cisco 7206VXR
Processor Memory	128 MB (default for NPE-225, NPE-400 and NSE-1) 256 MB (default for NPE-G1, max for NPE-225, NSE-1) 512 MB (max for NPE-400)	Same as Cisco 7204VXR
Flash disk memory card (optional, up to 2 slots available)	48 MB, expandable to 128 MB for I/O controllers 64 MB, expandable to 256 MB for NPE-G1	Same as Cisco 7204VXR

Network Management

Network Management Applications:
• Element Manager Software (EMS) for the Cisco 7200 and 7400 Series
• Cisco Secure Policy Manager
• Cisco VPN Device Manager (VDM)
• Cisco QoS Device Manager (QDM)
• Cisco Info Center
• CiscoWorks
• Secure command-line interface using Secure Shell (SSH) Protocol
• HTML-based management tool

Physical Specifications

Table 6

	Cisco 7204VXR	Cisco 7206VXR
Height	5.25 in. (13.34 cm)	5.25 in. (13.34 cm)
Width	16.8 in. (42.67 cm)	16.8 in. (42.67 cm)
Depth	17 in. (43.18 cm)	17 in. (43.18 cm)
Weight	Chassis is fully configured with a network processing engine, I/O controller, four port adapters, two power supplies, and a fan tray: ~50 lb (22.7 kg)	Chassis is fully configured with a network processing engine, I/O controller, six port adapters, two power supplies, and a fan tray: ~50 lb (22.7 kg)

Power

The Cisco 7200 is available with single and dual power supply options for both AC and DC.

Table 7

	Cisco 7204VXR	Cisco 7206VXR
AC-input power	370W max. (single or dual power supply configuration)	Same as Cisco 7204VXR
AC-input voltage rating	100–240 VAC wide input with power factor correction	Same as Cisco 7204VXR
AC-input current rating	Not to exceed 5A max. at 100 VAC and 2.5A max. at 240 VAC with the chassis fully configured	Same as Cisco 7204VXR
AC-input frequency rating	50/60 Hz	Same as Cisco 7204VXR

	Cisco 7204VXR	Cisco 7206VXR
AC-input cable	18 AWG 3-wire cable, with 3-lead IEC-320 receptacle on the power supply end, and a country-dependent plug on the power source end	Same as Cisco 7204VXR
DC-output power	280W max. (single or dual power supply configuration)	Same as Cisco 7204VXR
DC-input power	370W max. (single or dual power supply configuration)	Same as Cisco 7204VXR
DC-input voltage rating	–24 to –60 VDC for global DC power requirements	Same as Cisco 7204VXR
DC-input current rating	Not to exceed 13A max. at –48 VDC (370W/–48 VDC = 7.7A typical draw) Not to exceed 8A max. at –60 VDC (370W/–60 VDC = 6.2A typical draw)	Same as Cisco 7204VXR
DC voltages supplied and maximum steady-state current ratings	+5.2V at 36.0A +12.2V at 9A –12.0V at 1.5A +3.5V at 13A	Same as Cisco 7204VXR
DC-input cable	14 AWG recommended minimum, with at least 3 conductors rated for at least 140 F (60 C)	Same as Cisco 7204VXR
Frequency	50/60 Hz	Same as Cisco 7204VXR
Airflow	~80 cfm	Same as Cisco 7204VXR
Power dissipation	~370W max. configuration	Same as Cisco 7204VXR
Heat dissipation	370W (1262 BTUs)	Same as Cisco 7204VXR
Noise level	Front (I/O Controller and PA side):44.2 db Back (Power supply side): 43.7 db Left (Fan side): 47.2 db Right: 44.8 db	Same as Cisco 7204VXR

Protocols

The Cisco 7200 Series Router supports the following standard Internet protocols:

• *Layer 2 and Layer 3 protocols*—Address Resolution Protocol (ARP), IPCP, IP forwarding, IP host, IP Multicast, PPP-over-ATM, TCP, Telnet, Trivial File Transfer Protocol (TFTP), User Datagram Protocol (UDP), transparent bridging, virtual LAN (VLAN), MPLS, and IPv6.

• *Layer 3 routing protocols*—EIGRP, IGRP, IS-IS, OSPF, BGP, PIM, and RIP.

• *Network management and security*—AAA, CHAP, FTP, RADIUS, SNMP, PAP, and TACACS.

• RFC 1483: Multiprotocol Encapsulation over ATM AAL 5.
• RFC 1577: Classical IP and ARP over ATM AAL 5.

• *ARP*—Determines the destination MAC address of a host using its known IP address.

• *BOOTP*—Uses connectionless transport layer (UDP); allows the switch (BOOTP client) to get its IP address from a BOOTP server.

• *Internet Control Message Protocol (ICMP)*—Allows hosts to send error or control messages to other hosts; is a required part of IP; for example, the ping command uses ICMP echo requests to test if a destination is alive and reachable • *IP or IP over ATM*—Suite used to send IP datagram packets between nodes on the Internet.

• *TCP*—A reliable, full-duplex, connection-oriented end-to-end transport protocol running on top of IP; for example, the Telnet protocol uses the TCP/IP protocol suite.

• *Packet Internet groper (ping)*—Tests the accessibility of a remote site by sending it an ICMP echo request and waiting for a reply.

• *TFTP*—Downloads network software updates and configuration files (Flashcode) to workgroup switch products.

• *Reverse Address Resolution Protocol (RARP)*—Determines an IP address knowing only a MAC address; for example, BOOTP and RARP broadcast requests are used to get IP addresses from a BOOTP or RARPD server.

• *Serial Line Internet Protocol (SLIP)*—A version of IP that runs over serial links, allowing IP communications over the administrative interface.

• *PPP*—Provides host-to-network and switch-to-switch connections over synchronous and asynchronous circuits.

• *Simple Network Management Protocol (SNMP)*—Agents that process requests for network management stations and report exception conditions when they occur; requires access to information stored in a MIB.

• *Telnet*—A terminal emulation protocol that allows remote access to the administrative interface of a switch over the network (in-band)
• *UDP*—Enables an application (such as an SNMP agent) on one system to send a datagram to an application (a network management station using SNMP) on another system; uses IP to deliver datagrams; TFTP uses UDP/IP protocol suites.

• *Dynamic Host Connection Protocol (DHCP)*—Lets a host automatically obtain their IP address, subnet mask, and default route from a pre-configured DHCP server on the network.

• *Hot Standby Router Protocol (HSRP)*—Provides fast cut-over to a backup router in the event of a system or link failure.

Product Regulatory Approvals and Compliance

Product Regulatory Compliance

The following table lists regulatory compliance standards for the Cisco 7204VXR and 7206VXR chassis.

Table 8

	Compliance Standard
Product Safety	UL 1950, CSA 22.2 No. 950, EN60950, EN41003, AUSTEL TS001, AS/NZ 3260, IEC 950
Emissions	FCC Class A, CSA Class A, EN55022 Class B, VCCI Class 2, AS/NRZ 3548 Class A
Immunity	IEC-1000-4-2, IEC-1000-4-3, IEC-1000-4-4, IEC-1000-4-5, IEC-1000-4-6, IEC-1000-4-11, IEC-1000-3-2
NEBS	Level 3

Product System Requirements

Hardware Requirements

Hardware for Cisco 7200 Series Router includes:
• 7204VXR or Cisco 7206VXR chassis
• Network Processing Engine or Network Services Engine
• Input/Output controller
• Processor memory
• Input/Output controller memory
• Power supply
• Console and auxiliary cables
• Second power supply, accessories
• Port adapters
• Service adapters

Note: You must order a network processing or services engine for the Cisco 7206VXR and Cisco 7204VXR.With the NPE-225, NPE-400, and NSE-1 processors, you must also order an input/output controller. With the NPE-G1 processor, the input/output controller is optional.

Software Requirements

To locate the minimum supported Cisco IOS Software Release by train for all Cisco 7200 Series products, use the Hardware/Software Compatibility Matrix at: http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hwswmatrix.cgi. In general, the minimum support Cisco IOS Software releases for the Cisco 7204VXR and Cisco 7206VXR are 11.1(16)CA or later; 11.2(11)P or later; or 11.3(1) or later. Consult the compatibility matrix above for more detailed information.

Product Ordering Details

Ordering Instructions

Please visit http://www.cisco.com/public/ordering_info.shtml to place an order.

Product Part Number

To find part descriptions and part numbers for Cisco products, use the online Cisco Pricing Tool at: http://www.cisco.com/cgi-bin/front.x/pricing.

The base chassis product IDs are shown below. In addition, various bundles, spares, and options are available. To access part descriptions and part numbers use the online Cisco Pricing Tool at: http://www.cisco.com/cgi-bin/front.x/pricing.

Table 9

Part Number	Description
Cisco 7204VXR	Cisco 7204VXR, 4-slot chassis, 1 AC supply with IP software
Cisco 7206VXR	Cisco 7206VXR, 6-slot chassis, 1 AC supply with IP software

Migration Program

A Technology Migration Plan has been established for this product.
The Technology Migration Plan is an innovative, industry-first sales program that allows customers to trade in Cisco and competitors' products to receive a trade-in credit toward the purchase of any new Cisco product. The program underscores Cisco's commitment to its customers to provide end-to-end product solutions and effective migration options in the face of ever-changing network requirements.

For details about technology migration, go to:
http://www.cisco.com/offer/tic/TMP_PA.html

Service and Support

Cisco Systems offers a wide range of service and support options for its customers. More information on Cisco service and support programs and benefits are available at: http://www.cisco.com/public/Support_root.shtml.