PROPUESTA DE CONEXIÓN DE ENTORNOS IPv6 MEDIANTE UN BACKBONE MPLS/IPV4

Nancy Yaneth Gelvez García
Magister en Ciencias de la Información y las Comunicaciones
Docente planta de la Universidad Distrital Francisco José de Caldas
nygelvezg@udistrital.edu.co
Bogotá, Colombia

Danilo Alfonso López Sarmiento
Magister en Ciencias de la Información y las Comunicaciones
Docente planta de la Universidad Distrital Francisco José de Caldas
dalopezs@udistrital.edu.co
Bogotá, Colombia

Edwin Rivas Trujillo
Doctor en Ingeniería Eléctrica Electrónica y Automática
Docente planta de la Universidad Distrital Francisco José de Caldas
erivas@udistrital.edu.co
Bogotá, Colombia

Tipo: Artículo de investigación

Fecha de Recepción: Julio 8 de 2013
Fecha de Aceptación: Agosto 6 de 2013

PROPOSAL ON THE IPV6 CONNECTIONS OF ENVIRONMENTS BY USING AN MPLS/IPV4 BACKBONE

ABSTRACT
The current MPLS/IPv4 networks offer the advantage of implementing the traffic engineering, as well as performing the differentiation of flows based on the types of service (CoS) compared to networks with a traditional IP routing. In order to take advantage of the strategic qualities during the stage of coexistence between IPv4 and IPv6 there are 4 methods to provide connectivity to remote IPv6 Islands [1] through a Core MPLS along with a native IPv4 infrastructure [2], but one of the ways that allows a quick and easy provision of it based on the minimal requirements of the configuration and the equipment is to provide IPv6 tunnels through the network access (CE) routers. However, its four variables (Guide, GRE, 6to4 and IPv6 Compatible IPv4) [3] are appropriate or not according to the inherent characteristics of the network to interconnect; Therefore, this article presents the advantages and disadvantages of using each technique of "tunnelling".

Key words: automatic/dynamic tunnels, GNS3+dynamips, IPv6 isles, manual tunnels, MPLS IPv4 core.

RESUMEN
Las redes actuales MPLS/IPv4 presentan las ventajas de poder implementar ingeniería de tráfico, así como realizar diferenciación de flujos mediante clases de servicio (CoS) frente a las redes con enrutamiento IP tradicional. En aras de aprovechar cualidades estratégicas durante la etapa de coexistencia entre IPv4 e IPv6 existen 4 métodos para proveer conectividad a islas IPv6 [1] remotas a través de una infraestructura de core MPLS con IPv4 nativo [2], sin embargo una de las formas que permite un rápida y fácil provisión de la misma dados los mínimos requisitos de configuración y de equipos es la de disponer túneles IPv6 en los enrutadores de acceso (CE) de la red. No obstante, sus cuatro variantes (manual, GRE, 6to4 e IPv6 compatible IPv4) [3] resultan adecuadas o no según las características inherentes de la red a interconectar; por tanto este artículo presenta las ventajas y desventajas propias de la utilización de cada técnica de entunelamiento como resultado de la interconexión con los cuatro tipos de túneles de una red emulada mediante GNS3+Dynamips.

Palabras claves: core MPLS/IPv4, GNS3+dynamips, islas IPv6, túneles dinámicos/automáticos, túneles manuales.

1. INTRODUCCIÓN

Con el fin de contar con un servicio más robusto en cuanto a seguridad, la posibilidad de expandir sus capacidades exponencialmente sin restricciones ni limitaciones y contar con mayores prestaciones para sus usuarios, las empresas han empezado a centrar su atención en la migración de sus redes a unas soportadas por IPv6; sin embargo sus proveedores de red (SP o ISP) pueden de acuerdo a su capacidad, soportar o no este cambio inevitable de una forma sostenible, dependiendo de la estrategia utilizada para la interconexión.

No obstante, debido a que aún la mayoría de las redes de tales proveedores de servicio utilizan IPv4 nativo en su core (del tipo MPLS dadas sus ventajas frente al enrutamiento IP [19]), resulta conveniente utilizar un método de transición que permita tanto el tráfico de IPv4 como de IPv6 durante la migración definitiva a IPv6.

Por tanto, con el objetivo de aprovechar las ventajas de una red de core MPLS/IPv4 (entre las que se cuentan la capacidad de realizar ingeniería de tráfico y la diferenciación de tráfico mediante CoS [19]) para proveer conectividad IPv6, existen 4 métodos de interconexión de islas IPv6 [2], los cuales son:

- Túneles IPv6 en los enrutadores de acceso (CE).
- IPv6 sobre MPLS con circuitos de transporte.
- IPv6 en los enrutadores de distribución (PE) o 6PE.
- Adicionar VPN's IPv6 sobre MPLS a los 6PE (conocido como 6VPE).

Dichas posibilidades de interconexión de islas IPv6 a través de una infraestructura de core MPLS IPv4, surgen como alternativas a la migración de la red de forma completa a IPv6 (lo cual no es recomendable durante la transición IPv4 IPv6 al imposibilitar el tráfico IPv4 a través de la misma) y por tanto una vez comienzan a aumentar el número de usuarios IPv6 nativos se debe pensar en realizar tal migración (o cambiar la red a una de doble pila) [5]; sin embargo, durante las etapas tempranas de la transición a IPv6 la interconexión mediante túneles resulta la solución de más sencilla implementación debido a su fácil configuración y requerimientos de red (no necesita de PE's doble pila como en el caso de 6PE y 6VPE, sino sólo de CE's de este tipo). A pesar de las facilidades para la interconexión IPv6 a partir de Túneles en los CE de la red, esta técnica dificulta el diagnóstico de fallas en la red, dado que no permite la utilización de trazados de ruta en la red.

El presente artículo pretende dar a conocer los resultados encontrados al desplegar redes IPv6 a través de una infraestructura de core MPLS IPv4, así como determinar las ventajas y desventajas de las diferentes técnicas de entunelamiento, a partir de la interconexión de una red de prueba mediante las 4 variantes de túneling IPv6 en los CE mediante el emulador GNS3+Dynamips.

2. INTERCONEXIÓN DE ISLAS IPV6 SOBRE UN CORE MPLS/IPv4

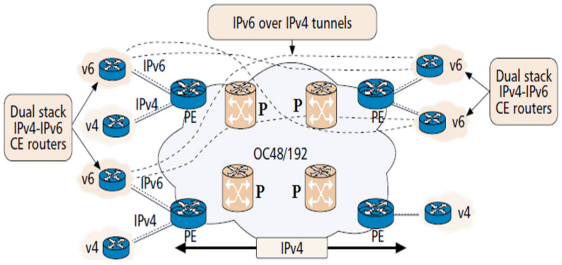


Figura 1. Túneles IPv6 en los enrutadores de acceso CE [2]

El primer método (figura 1) consiste en el tendido de túneles en los enrutadores de acceso doble pila (soportan IPv6 como IPv4), permitiendo el tráfico IPv6 de forma transparente para el core MPLS (conformado por los enrutadores P y PE) de la red al encapsular los paquetes IPv6 en IPv4.

El segundo método interconecta las islas IPv6 mediante enlaces dedicados que son transparentes para IPv6 y por tanto la infraestructura de core nativo MPLS/IPv4 no requiere de modificaciones en su estructura. El tráfico IPv6 se transporta a través de túneles que utilizan

las capacidades "cualquier transporte sobre MPLS" (AToM) o "ethernet sobre MPLS" (EoMPLS, figura 2), por tanto son mandatorias las conexiones ATM o ethernet respectivamente entre el proveedor y los enrutadores de acceso.

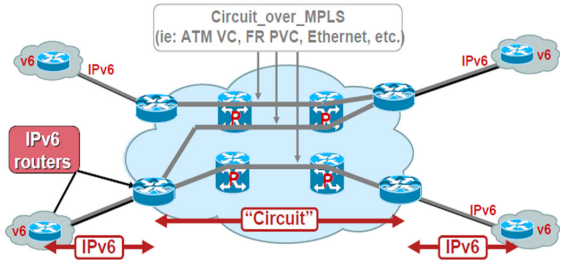


Figura 2. IPv6 sobre MPLS con circuitos de transporte [2]

El tercer método (figura 3) aprovecha en el PE las extensiones multiprotocolo de BGP (Multiprotocol Border Gateway Protocol, MP-BGP [5] [6]) para intercambiar información de ruteo IPv6. Los enrutadores PE son configurados para soportar tanto IPv4 como IPv6 (doble pila), y el uso de direcciones IPv6 mapeadas IPv4 (de la forma ::FFFF:100.200.120.45) con las que se intercambian prefijos de ruteo IPv6.

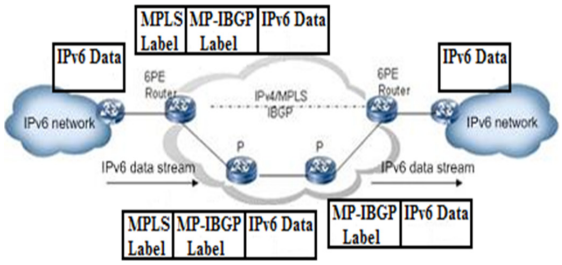


Figura 3. IPv6 en los enrutadores de distribución (6PE) [7]

En los enrutadores PE (nombrados como 6PE al utilizar esta solución) de ingreso se impone una jerarquía de etiquetas para hacer el tráfico IPv6 transparente para los enrutadores de core. Una primera etiqueta (MPLS Label) provee conectividad dentro del core MPLS IPv4, la cual se distribuye por LDP (Protocolo de Distribución de Etiquetas), TDP (Protocolo de Distribución de "Rótulos" -Tags-) o RSVP (Protocolo de Reservación de Recursos) en caso de intercambio de etiquetas MPLS-TE (MPLS con ingeniería de tráfico). Una segunda etiqueta (MP-IBGP Label), automáticamente asignada al prefijo IPv6 de destino es distribuida por BGP multiprotocolo y usado en cada enrutador 6PE de salida para la transmisión IPv6.

6PE conecta todas las redes IPv6 a través de una única VPN, por lo que no pueden ser separadas lógicamente. Para realizar dicha separación las redes IPv6 conectadas (es decir hacer uso de VPN IPv6) se debe entonces utilizar 6VPE.

El último método (6VPE, figura 4) es una extensión de la tecnología MPLS VPN para IPv6, la cual puede ofrecer servicios de VNP IPv4 o IPv6 a través de redes de core MPLS IPv4 o IPv6, adicionando al método anterior los conceptos de address family y VRF-IPv6, aumentando así la seguridad de las islas IPv6 a interconectar.

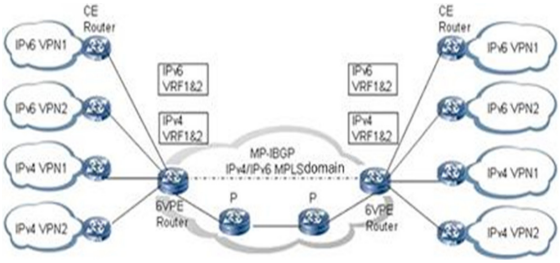


Figura 4. IPv6 VPN en los PE de la red (6VPE) [4]

Existen 4 variantes de la técnica de entunelamiento IPv6 [3] (realmente 5 con ISATAP [8], aunque esta permite únicamente el tráfico IPv6 dentro de una misma Isla IPv6 y no entre diferentes islas IPv6), las cuales se dividen en dos:

- Manuales (o punto a punto): manual [9] y GRE [10].
- Automáticos/dinámicos (o punto a multipunto): 6to4 [11] e IPv6 compatible IPv4 [9].

2.1. Túneles IPv6 manuales

Un túnel manual es equivalente a un link permanente entre dos dominios (islas) IPv6 sobre un core IPv4 [7]. Su uso primario son conexiones estables que requieren una comunicación continua y segura entre dos enrutadores de acceso, o entre un sistema final y un enrutador de acceso, o para interconectar islas IPv6.

Túnel manual: se debe configurar una dirección IPv6 manualmente en una interface túnel, así como una dirección IPv4 al inicio y al final del túnel.

Túnel GRE (encapsulación de ruteo genérica): estos túneles no están ligados a un protocolo pasajero o de transporte específico, pero en este caso llevan IPv6 como protocolo pasajero (puede ser IPv6 o IS-IS), con GRE como el protocolo portador.

2.2. Túneles IPv6 automáticos/dinámicos

Los túneles automáticos proveen una interconexión punto a multipunto (a diferencia de los dos anteriores, los cuales eran punto a punto). Este tipo de túneles no utiliza una configuración por pares de enrutadores, debido a que trata la infraestructura IPv4 como un link virtual multiacceso sin difusión. La dirección IPv4 embebida en la dirección IPv6 es utilizada para encontrar el otro extremo del túnel automático.

Túneles 6to4: el destino del túnel es determinado por la dirección IPv4 del enrutador de distribución (conectada al de acceso, CE), extraída de la dirección IPv6 que comienza con el prefijo 2002::/16, y que contiene la IPv4 embebida (convertida a hexadecimal y ubicada en a partir del bit 17 hasta el 48 de la dirección IPv6) designada como fuente del túnel. Los 16 bits siguientes a la dirección IPv4 embebida, se usan para numerar redes dentro de la isla IPv6. Cada isla IPv6 debe tener como requisito una IPv4 única globalmente en caso de necesitar conectarse a Internet.

Túneles IPv6 compatibles IPv4: este tipo de túneles utiliza direcciones IPv6 compatibles con IPv4. Esta técnica usa la dirección IPv4 expuesta para determinar el destino del túnel y es del tipo punto a multipunto. En [12] se estipula la ya no obligatoriedad de la compatibilidad con este tipo de direcciones (reemplazada por las direcciones IPv6 mapeadas IPv4) y este tipo de túneles rara vez se debiera utilizar (se recomienda 6to4), debido al direccionamiento limitado de este método de ser necesaria la conexión a Internet (requiere de direcciones IPv4 globalmente únicas) [13].

Cabe mencionar que los túneles automáticos (a diferencia de los de tipo manual [manual y GRE]) inhiben el uso de las capacidades de anycast y multicast de IPv6 en la red.

3. DISEÑO DE LA TOPOLOGÍA DE PRUEBA

Siguiendo con el esquema de diseño de tres capas (core, distribución y acceso), se propone valuar las técnicas anteriormente mencionadas mediante la interconexión de cinco islas IPv6 (redes 11::/64, 22::/64, 33::/64, 44::/64, 55::/64) interconectadas respectivamente a través de interfaces FastEthernet [con direcciones IPv6 manualmente configuradas: 11::11:1/64, 22::22:2/64, 33::33:3/64, 44::44:4/64 y 55::55:5/64] en CE1, CE2, CE3, CE4 y CE5), que conforman la capa de acceso.

Dadas las similitudes entre los túneles manuales y GRE, se les asignó el mismo direccionamiento y protocolo de ruteo IPv6; y de forma similar con los túneles 6to4 e IPv6 compatibles IPv4, con el mismo protocolo de routing IPv6.

3.1. Infraestructura MPLS/IPv4 para la interconexión de las islas IPv6

Para proveer conectividad nativa IPv4 a las sedes se dispuso de tres enrutadores de distribución (PE1, PE2 y PE3; es decir enrutadores de borde del proveedor, los cuales son el punto de ingreso a la nube IPv4/MPLS) y dos enrutadores de core (P1 y P2); que hacen las veces de nodos LSRs en el segmento rectangular central detallado en la figura 5.

Las interconexiones entre los cinco enrutadores de acceso y los tres de distribución se emularon mediante enlaces seriales con un reloj de 128 Kbps configurados en los enrutadores de distribución (DCE) y con encapsulación PPP. Las interconexiones MPLS entre los enrutadores de core y distribución se emularon por medio de enlaces GigaEthernet con LDP para la distribución de etiquetas MPLS (se utilizó LDP, aunque en caso de implementarse MPLS-TE también permite RSVP).

3.2. Esquema de direccionamiento y protocolos de ruteo IPv4 en la red

Se utilizó un direccionamiento privado para el core (P1 y P2) y distribución (PE1, PE2 y PE3) MPLS con 5 redes /30, comenzando con 172.16.1.0/30 hasta la 172.16.1.16/30. De forma similar se numeraron las conexiones WAN (enlace entre distribución y acceso), mediante 5 redes /30, a partir de 192.168.100.0/30 hasta 192.168.100.16/30. Finalmente se le asignó una dirección de Loopback a los 5 CE (192.168.255.<1-5>/32) a los 3 PE (172.20.20.<3-5>/32) y a los 2 P (172.20.20.<1-2>/32).

Se escogió OSPF como protocolo de ruteo IPv4 de la red buscando así no limitar el tipo de nodos en la red (a sólo Cisco con EIGRP) y al mismo tiempo asegurando la escalabilidad de la red.

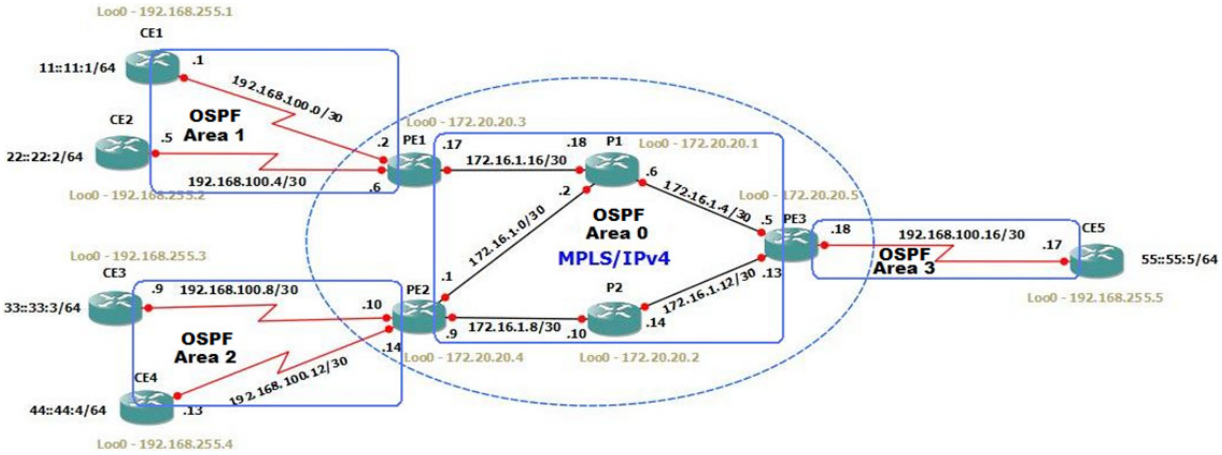


Figura 5. Topología de prueba y segmentación OSPF multiárea de la red para la interconexión de islas IPv6 mediante las diferentes técnicas de entunelamiento [4].

3.3. Esquema de direccionamiento y protocolos de ruteo IPv6 en la red

3.3.1. Túneles manuales (manual y GRE)

Para el caso de la interconexión manual y GRE, donde se debe especificar tanto una dirección fuente como una de destino en cada túnel; se utilizaron las IP de Loopback de cada CE. Además es necesaria la asignación de una dirección IPv6 a cada extremo de los túneles; y ya que con este tipo de solución para la interconexión es necesaria la creación de un túnel en cada CE (2 por el par de islas a interconectar), fue necesaria la configuración de 20 direcciones IPv6 (tabla 1).

Particularmente para conocer el número de túneles manuales (o GRE) para interconectar determinado número de islas IPv6 se puede utilizar la ecuación (1).

$$\#Tuneles = n \cdot (n-1) \qquad (1)$$
$$\#Tuneles = \#IPv6\ Adicionales$$

Donde n es el número de islas IPv6 a interconectar. Las direcciones IPv6 configuradas en los extremos de cada túnel se muestran en la tabla 1.

Con la asignación de los túneles se pretende conocer los CE conectados (ej. Tunnel12 conecta el CE1 con CE2).

Ya que para los IOS un túnel es considerado como un enlace IPv6 (tal como un enlace ethernet, serial, etc), se puede correr cualquier protocolo de ruteo IPv6 soportado por el IOS sobre el túnel manual (manual y GRE). En el caso de IS-ISv6, sólo es soportado mediante GRE [14] sin mecanismos adicionales, o bien haciendo uso de BGP4+ en cualquiera de las técnicas de entunelamiento.

Tabla 1. Esquema de direccionamiento IPv6 utilizado en los Túneles Manuales y GRE

Router	# de Túnel	IPv6 asignada
CE1	Tunnel12	12::12:1/64
CE1	Tunnel13	13::13:1/64
CE1	Tunnel14	14::14:1/64
CE1	Tunnel15	15::15:1/64
CE2	Tunnel12	12::12:2/64
CE2	Tunnel23	23::23:2/64
CE2	Tunnel24	24::24:2/64
CE2	Tunnel25	25::25:2/64
CE3	Tunnel13	13::13:3/64
CE3	Tunnel23	23::23:3/64
CE3	Tunnel34	34::34:3/64
CE3	Tunnel35	35::35:3/64
CE4	Tunnel14	14::14:4/64
CE4	Tunnel24	24::24:4/64
CE4	Tunnel34	34::34:4/64
CE4	Tunnel45	45::45:4/64
CE5	Tunnel15	15::15:5/64
CE5	Tunnel25	25::25:5/64
CE5	Tunnel35	35::35:5/64
CE5	Tunnel45	45::45:5/64

Conocidas ya las razones de la selección de OSPF como protocolo de ruteo IPv4 en la red, y en aras de estandarizar toda la red diseñada, se optó por OSPFv3 como protocolo de ruteo IPv6 en la red, el cual se configuró en dos áreas, así (figura 6).

- Área 0 en las interfaces túnel configuradas.
- Área 1 en las interfaces FastEthernet de los CE's.

A continuación se muestra el equivalente punto a punto IPv6 entre CE1 y CE2, así como la asignación de áreas para OSPFv3 de acuerdo con el esquema de direccionamiento en la tabla 1 para el caso de túneles manuales y GRE.

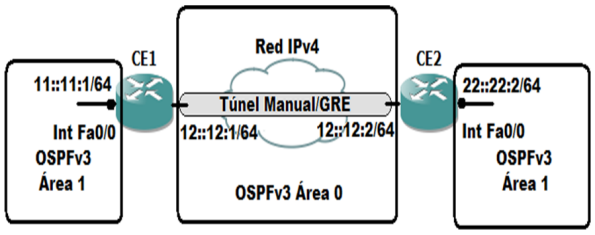


Figura 6. Equivalente IPv6 y segmentación OSPFv3 multiárea de la red del túnel 12 entre CE1 y CE2

3.3.2. Túneles automáticos/dinámicos (6to4 e IPv6 compatibles IPv4)

Para este tipo de solución, en la que los túneles son ahora punto a multipunto, no es necesario configurar un mayado de *n(n-1)* túneles (como en el caso de túneles punto a punto, ecuación (1)) para la interconexión de n islas IPv6 debido a la naturaleza de este tipo de túneles, sino únicamente n túneles, los cuales requieren una dirección fuente IPv4 (en este caso y usualmente para tales fines, la dirección IP de Loopback de los CE), y hacen uso de las direcciones IPv4 embebidas en IPv6 de la dirección de destino (pertenecientes al prefijo 2002::/16 en el caso de 6to4 y al prefijo 0::/96 para IPv6 compatible IPv4) para encontrar el otro extremo del túnel dinámico.

Las direcciones IPv6 configuradas (para el caso de la solución con túneles 6to4) y las direcciones automáticas (en el caso de la solución con túneles IPv6 Compatibles IPv4) para cada uno de los túneles configurados (5 túneles, uno por cada isla IPv6 a interconectar) se muestran en la tabla 2 y 3.

Tabla 2. Esquema de direccionamiento IPv6 utilizado en la solución con túneles 6to4

Router	Loopback/Fuente Túnel	Dirección IPv6
CE1	192.168.255.1/32	2002:C0A8:FF01::/45
CE2	192.168.255.2/32	2002:C0A8:FF02::/45
CE3	192.168.255.3/32	2002:C0A8:FF03::/45
CE4	192.168.255.4/32	2002:C0A8:FF04::/45
CE5	192.168.255.5/32	2002:C0A8:FF05::/45

Tabla 3. Esquema de direccionamiento IPv6 de la solución con túneles IPv6 compatibles IPv4

Router	Loopback/Fuente Túnel	Dirección IPv6
CE1	192.168.255.1/32	:: 192.168.255.1/96
CE2	192.168.255.2/32	:: 192.168.255.2/96
CE3	192.168.255.3/32	:: 192.168.255.3/96
CE4	192.168.255.4/32	:: 192.168.255.4/96
CE5	192.168.255.5/32	:: 192.168.255.5/96

Cabe destacar que el segundo y tercer cuarteto de las direcciones IPv6 asignadas en la solución con túneles 6to4 son el resultado de la conversión de las direcciones fuente de cada túnel (en este caso las de Loopback) a hexadecimal, y el prefijo /45 se debe al número de bits en binario iguales de las direcciones fuente de los túneles a que harán parte de la solución, siendo este el mayor prefijo conectado para proveer conectividad a las cinco IPv6 relativas a la solución (también es posible la asignación de los prefijos menos específicos como /44, /43, etc.).

Dado que los IGP's (Interior Gateway Protocols) IPv6 como OSPFv3, RIPng intercambian actualizaciones de ruteo entre las interfaces Link Local IPv6, su utilización directa en los túneles dinámicos no es posible debido a las direcciones IPv6 derivadas de IPv4 utilizadas tanto en 6to4 como con túneles IPv6 compatibles IPv4. Por lo tanto, para proveer ruteo dinámico a los escenarios con túneles dinámicos, se debe hacer uso de BGP (cuyos procesos de ruteo utilizan pares TCP establecidos entre cualquier dirección IPv6 para intercambiar actualizaciones). A pesar de que las soluciones dinámicas, además de funcionar mediante BGP4+ (Extensiones Multiprotocolo de BGP) [15] [16], funcionan con rutas por default, se optó por implementar la solución con BGP4+ y distribuir rutas de OSPFv3 en cada CE (más precisamente en las interfaces LAN/FastEthernet de los CE's), con el fin de contar con las ventajas del ruteo dinámico para los dos escenarios de interconexión mediante túneles dinámicos.

De acuerdo a lo anteriormente expuesto, se configuró cada CE como un sistema autónomo (AS) comenzando por el 65001 para CE1 hasta 65005 para CE5 (tabla 4).

Tabla 4. AS's configurados en los CE's para las soluciones de túneles dinámicos (6to4 e IPv6 compatible IPv4)

Router	Sistema Autónomo
CE1	65001
CE2	65002
CE3	65003
CE4	65004
CE5	65005

A continuación se muestra el equivalente IPv6 (omitiendo las direcciones IPv6 de los túneles) para CE1 y CE2 de la topología diseñada para las soluciones con túneles dinámicos de acuerdo a la asignación de AS's en la tabla 4 y mostrando la vecindad EBGP a través de la cual se distribuyen rutas de OSPFv3 del área 1 (figura 7).

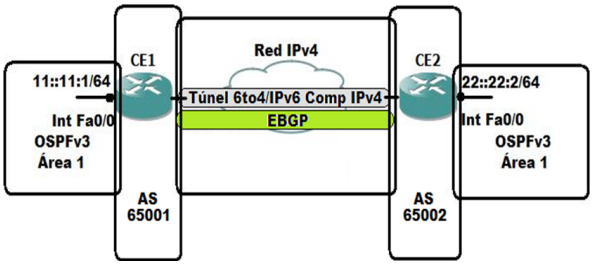


Figura 7. Segmentación en AS's de la red para las soluciones con túneles dinámicos entre CE1 y CE2

Cabe resaltar que respecto de la solución con túneles manuales (manual y GRE), ya no se puede utilizar OSPF en el túnel (ahora dinámico), sino que en cambio se define cada CE como un sistema autónomo (AS), el cual distribuye OSPF (en este caso el área 1) con sus pares TCP (CE's restantes) mediante BGP4+.

4. ANÁLISIS DE RESULTADOS

De acuerdo a los 4 escenarios propuestos, interconexión con túneles manuales, GRE, 6to4 e IPv6 Compatible IPv4 sobre la red MPLS/IPV4 de core, al implementarse, fueron utilizados 2 tipos de enrutadores soportados por GNS3+Dynamips; los cuales fueron el

Cisco 3745 (con IOS c3745-adventerprisek9-mz.124-18.bin) para los 5 enrutadores de acceso (CE's) y el Cisco 7206VXR NPE-400 (con IOS c7200-jk9s-mz.124-13b.bin) para los 5 enrutadores de core + distribución (2 de core [P1 y P2] y 3 de distribución [PE's]).

En cuanto a requerimientos de configuración fue necesario el uso de 20 túneles manuales y GRE (reemplazar n por 5 en la ecuación (1)) frente a los 5 túneles 6to4 e IPv6 compatibles IPv4 para garantizar la conectividad de las cinco islas IPv6 dispuestas en la topología de prueba.

Haciendo uso de los accesos por consola a los CE se realizaron pruebas de ping IPv4 (2000 repeticiones con tamaño de 100 bytes) a las direcciones de Loopback de cada uno de los sitios remotos tomando como dirección fuente la dirección de Loopback del propio CE, así como pruebas de ping IPv6 (2000 repeticiones con tamaño de 1280 bytes (mínimo tamaño de link MTU)) a las LAN (FastEthernet0/0) de cada sitio remoto tomando como dirección fuente la LAN de cada CE. A continuación se muestran los resultados de dichas pruebas (realizadas 2 veces) para el caso del enrutador CE1 (en las cuatro topologías implementadas).

Tabla 5. Resultados de latencia y porcentaje de éxito para las pruebas de ping en los 4 escenarios implementados

	Latencia IPv4 (ms)/Success Rate (%)		Latencia IPv6 (ms)/Success Rate (%)	
Técnica Tunneling	Loo2Loo 2 Saltos	Loo2Loo 4 Saltos	LAN2LAN 2 Saltos	LAN2LAN 4 Saltos
Manual	74.5/100	148.66/100	79/100	157.83/100
GRE	74/100	147.33/100	72.5/100	146.5/100
Media Manuales	**74.25/100**	**148/100**	**75.75/100**	**152.16/100**
6to4	75.5/100	151.5/100	88/100	172.83/100
IPv6 comp. IPv4	76/100	152.66/100	88/100	173/100
Media Automát	**75.75/100**	**152.08/100**	**88/100**	**172.91/100**

Se realizaron 2000 y 6000 repeticiones en los ping (Loopback a Loopback + LAN a LAN) de 2 Saltos y 4 Saltos respectivamente (entre CE1 y CE2, y entre CE1 y: CE3, CE4 y CE5).

De acuerdo a la tabla 5, las 4 soluciones tienen una gran estabilidad (no presentan pérdidas de paquetes), así como una mayor latencia IPv6 en promedio (172.91 ms de tiempo de ida y vuelta para los destinos con 4 saltos entre sus extremos en el caso de las soluciones con túneles automáticos frente a los presentados con las implementaciones manuales (manual y GRE, con 157.83ms y 146.5ms de RTT respectivamente). Cabe mencionar que las soluciones automáticas (6to4 e IPv6 compatible IPv4) tienen una latencia similar, mientras que dentro de las técnicas manuales, GRE tiene latencias IPv6 menores en un 8% comparadas con las obtenidas a partir de túneles manuales (146.5ms vs 157.83ms).

Además se observó que la red IPv4 en general, sin importar la solución de entunelamiento implementada conserva una latencia promedio de 150,03 ms (148.66 ms para el caso Manual, 147.33 ms para el caso de GRE, 151.5 ms para el caso 6To4 y 152.66ms con túneles IPv6 compatibles IPv4), tal y como se esperaría al ser la misma configuración IPv4 para los 4 casos implementados.

Para identificar el overhead asociado a cada técnica utilizada, el cual corresponde con los bits adicionales al campo de datos para la transmisión de paquetes en una red, en este caso para posibilitar el tráfico IPv6 a través de una red IPv4 por medio del mecanismo de encapsulación (reduciendo tanto la velocidad de transmisión como el máximo tamaño de los paquetes en la red o MTU), se realizó una captura de paquetes durante las pruebas de ping y posterior análisis con Wireshark, donde se observó que los túneles GRE a diferencia de los otros tres tipos de túneles adiciona un mayor over-

head (figura 8) (24 bytes por paquete haciendo uso de GRE frente a 20 bytes de los demás túneles), debido a la encapsulación adicional (4 bytes correspondientes al header GRE [Campos Banderas + Versión = 2 bytes y Protocolo = 2 bytes]).

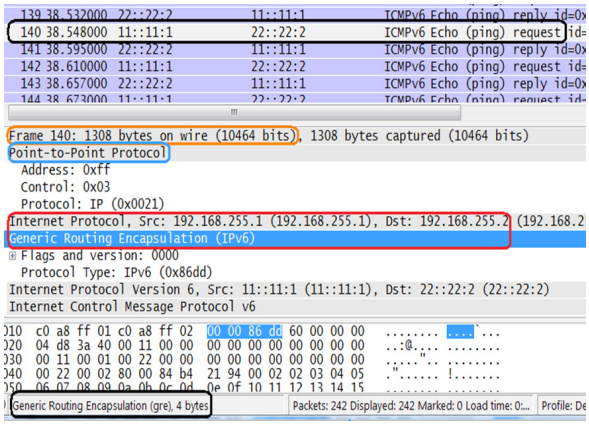


Figura 8. Captura a nivel de WAN en CE1 mediante Wireshark del tráfico IPv6 para la solución con GRE

En la figura 8 se detalla en el rectángulo negro superior un paquete de ping IPv6 (ICMPv6) con dirección fuente 11::11:1 y dirección destino 22::22:2; en el rectángulo naranja el tamaño total del paquete, en este caso 1308 bytes, correspondientes en su orden a PPP (4 bytes, rectángulo azul), Header IP (20 bytes, rectángulo rojo), GRE (4 bytes, rectángulo rojo y detalle del tamaño en el rectángulo negro inferior), Header IPv6 (40 bytes) e ICMPv6 (1240 bytes), esto con pings de 1280 bytes de tamaño; en el rectángulo rojo se detalla el overhead debido a los túneles GRE (encapsulación IP + GRE), donde se observa además que las direcciones fuente 192.168.255.1 y destino 192.168.255.2 coinciden con las direcciones de Loopback (direcciones fuente y destino del túnel 12) de los CE 1 y 2.

Con un análisis similar al realizado anteriormente mediante Wireshark, se aumentó el tamaño de ping en la red hasta observar la fragmentación de los paquetes, con lo cual se verificó el mayor MTU antes de tener que fragmentar en los enlaces seriales, encontrándose que con el overhead debido a los túneles configurados, tal MTU se reduce en 28 bytes en el caso de hacer uso de GRE (1500 bytes – [24 bytes + 4 bytes] = 1472 bytes; descontando los 4 bytes debidos a PPP) y en 24 bytes en el caso de las demás técnicas de entunelamiento implementadas (dejando un MTU de 1476 bytes).

Debido a que no es posible la generación de tráfico más allá del generado mediante pings en la red (lo cual no permite la saturación de los enlaces), no se incluyeron gráficas relacionadas con la carga en los enlaces, sin embargo, conocido el overhead asociado a cada técnica de entunelamiento implementada se puede tener una previsión del ancho de banda IPv6 consumido respecto de un tamaño de paquetes, el cual tendrá un rango desde 1280 bytes (mínimo link MTU IPv6) hasta 1472 bytes haciendo uso de GRE y de 1476 bytes con las demás técnicas de entunelamiento trabajadas, asegurando así la no fragmentación de paquetes en la red (en caso de presentarse, el rendimiento de la red se disminuye al tener que transmitir en 2 paquetes el paquete que podría ser enviado en 1, teniendo así unos tiempos de respuesta mayores, así como un mayor tráfico en la red asociado a overhead).

Tabla 6. Porcentaje de tráfico técnicas de túneles

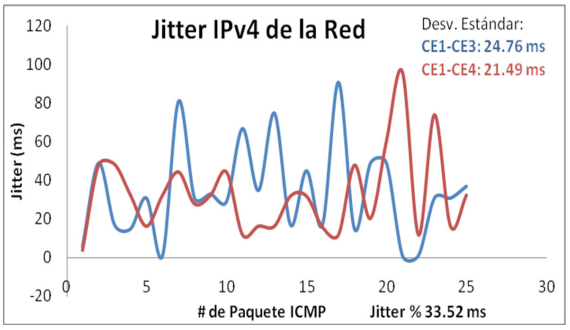
MTU (bytes)	Manual	GRE	6to4	IPv6 comp. Ipv4
1280	24/1.875	28/2.1875	24/1.875	24/1.875
1472	-	28/1.9	-	-
1476	24/1.626	-	24/1.626	24/1.626

En la tabla 6 se observa que el tráfico debido al overhead junto con PPP representa en el peor de los casos (mínimo MTU) un porcentaje de 2,18% haciendo uso de GRE y un 1,8% con las demás técnicas; hasta llegar al 1,9% y 1,6% con GRE y las demás técnicas respectivamente, lo cual en caso de saturación del enlace (en este caso 128 Kbps) resulta en una reducción del tráfico de entre 2,8 Kbps y 2,4 Kbps con GRE y de entre 2,3 Kbps y 2 Kbps con las demás técnicas de entunelamiento trabajadas.

Si bien la utilización de GRE genera una reducción de tráfico de 0,2% adicional respecto de

las demás técnicas de entunelamiento, permite tener unas redes más seguras al contar los paquetes con una encapsulación adicional que puede reducir significativamente los ataques de suplantación (spoofing) que se pudieran presentar, así como contar con la capacidad de autenticación.

Por último, se realizaron mediciones del jitter en la red a partir de un debug en CE1 durante la realización de pruebas de ping IPv4 (50 paquetes de 100 bytes, 25 hacia CE3 [líneas de tendencia azules] y 25 hacia CE4 [líneas de tendencia rojas] en la red sin entunelamiento implementado) e IPv6 (50 paquetes de 1280 bytes, 25 y 25 hacia CE3 y CE4 respectivamente para cada técnica de entunelamiento). A continuación se muestran las gráficas de jitter, así como un resumen con el jitter mínimo (tabla 7), promedio y máximo de acuerdo a la figura 9.



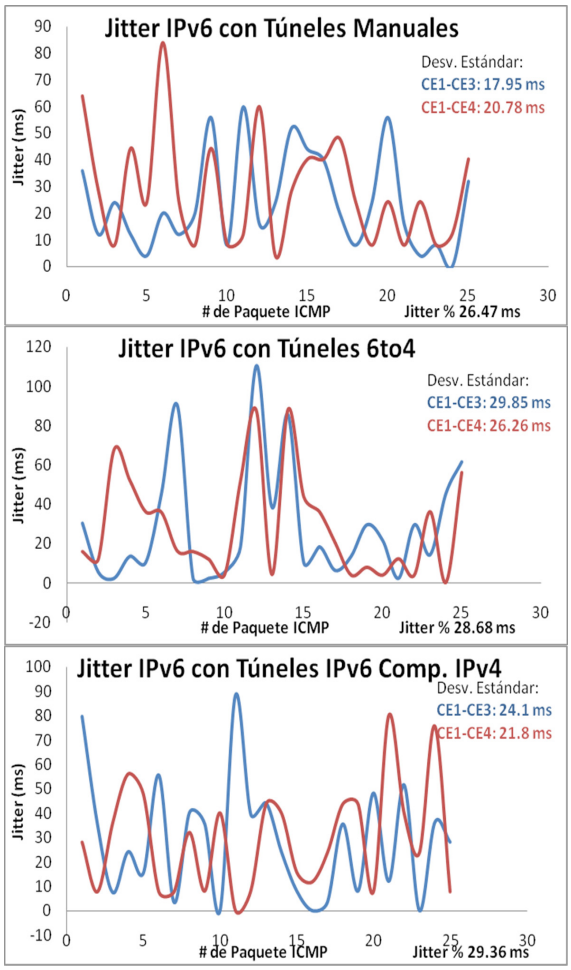


Figura 9. Variación del retardo para IPv4 como IPv6 para cada escenario implementadoentre CE1 y; CE3 (series azules) y CE4 (series rojas)

Tabla 7. Variación del retardo mínimo, promedio y máximo IPv4 e IPv6 en la red interconectada con las diferentes técnicas de entunelamiento

	Jitter IPv4 (ms)			Jitter IPv6 (ms)		
Técnica Tunneling	Mínimo	Promedio	Máximo	Mínimo	Promedio	Máximo
Manual	1,08	33,5296	95,76	0	26,4768	83,84
GRE				1,12	24,8864	67,48
6t04				0,16	28,7808	110,4
IPv6 com. IPv4				0,16	29,3696	88,32

Se observa que el jitter promedio IPv6 es menor al promedio IPv4 en la red; GRE presenta los jitter IPv6 promedio y máximo menores en comparación con las demás técnicas de entunelamiento, seguido por la interconexión manual, 6to4 e IPv6 compatible IPv4 (de estos dos últimos con un peor jitter IPv6 máximo para 6to4); sin embargo todos los valores de Jitter promedio IPv6 se encuentran dentro del rango recomendado de 100ms para VoIP en un solo

sentido en la red (con el fin de ser compensado efectivamente en el receptor mediante el uso de búferes jitter [17]). Cabe resaltar que los valores obtenidos fueron resultado de la comparación en los tiempos de ida y vuelta en la red, lo cual indica que en el mejor de los casos el jitter en un sentido sería la mitad de los valores obtenidos (es decir, con un aporte igual en el recorrido de ida como de vuelta al jitter total).

Finalmente se observa que en las gráficas de la figura 9 la variación del retardo tiene un comportamiento en su mayor parte del tipo transiente [18], asociado al intercambio de información de ruteo, y caracterizado por variaciones substanciales en su magnitud y que afectan a no más de un paquete de forma consecutiva; además del hecho de que la dispersión del jitter respecto del promedio (desviación estándar) en la red con paquetes IPv4 se reduce al hacer uso de túneles manuales y GRE, mientras que con túneles IPv6 compatible IPv4 se logra un comportamiento similar y al utilizar túneles 6to4 se empeora tal parámetro.

5. CONCLUSIONES

En general, las implementaciones de las soluciones de interconexión de islas IPv6 mediante túneles dinámicos (6to4 e IPv6 Compatible IPv4) y ruteo dinámico (que soporten de BGP4+) requieren de enrutadores CE de mayor gama y por tanto resultan ser una solución más cara a la hora de ser implementada en redes reales, frente a las soluciones de interconexión con túneles manuales (manual y GRE) y túneles dinámicos con ruteo estático.

La utilización de túneles dinámicos (6to4 e IPv6 compatible IPv4) para la interconexión de islas IPv6 a través de redes IPv4 resulta comparativamente mejor en cuanto a configuración a medida que aumenta el número de islas a interconectar frente a las técnicas de túneles manuales (manual y GRE), y para el caso de la red utilizada, fueron necesarios 4 veces el número de túneles configurados manualmente frente a aquellos de naturaleza dinámica (20 manuales y 5 dinámicos) para la interconexión de 5 islas IPv6.

Los túneles IPv6 compatibles IPv4 resultan más fáciles de implementar en cuanto a configuración frente a los túneles 6to4, debido a que de forma automática construyen su dirección IPv6 (dirección IPv6 compatible IPv4) a partir de su dirección IPv4 asignada como fuente en cada túnel, mientras que en la técnica 6to4 se requiere la configuración manual de dicha dirección IPv6 a partir de la conversión a hexadecimal de la dirección IPv4 configurada como fuente en cada túnel y calcular el prefijo de la dirección IPv6 a partir de los bits iguales en las direcciones fuente de los túneles en las islas IPv6 a interconectar. A pesar de esta ventaja en cuanto a configuración esta técnica es rara vez usada en la práctica, prefiriéndose la técnica de 6to4, que a pesar de también necesitar direcciones IPv4 globalmente únicas de requerirse la conexión a Internet, permite la numeración de subredes (16 bits) y hosts (64 bits); razón por la cual el tipo de dirección IPv6 utilizada en esta técnica no es recomendada a partir del RFC 4291 y se reemplaza por direcciones del tipo IPv6 mapeadas IPv4 (utilizadas en 6PE y 6VPE).

En caso de que las islas IPv6 utilicen IS-ISv6 como protocolo de ruteo interno, únicamente la solución con túneles GRE admite la interconexión sin mecanismos adicionales; esto ya que permite especificar IS-IS como protocolo pasajero (tal como se hace con IPv6) y por tanto se pueden transportar ambos, IS-IS e IPv6 al mismo tiempo sobre el mismo túnel. En caso de utilizar las extensiones multiprotocolo de BGP (BGP4+) cualquier técnica de entunelamiento soporta IS-IS como protocolo de ruteo IPv6.

A pesar de la limitante de escalabilidad propia de las soluciones con túneles manuales (manual y GRE); se puede superar este impedimento si en vez de configurar los túneles en cada uno de los enrutadores de Acceso de la red (CE's) se realizase tal configuración en los enrutadores de distribución (PE's), reduciendo así el número de túneles a $m(m-1)$ túneles, siendo m el número de enrutadores de distribución en la red (PE's), sin importar el número de islas IPv6 a interconectar (en el caso de la topología propuesta, para la interconexión de las 5 islas IPv6

sería necesaria la configuración de únicamente 6 túneles, debido a los 3 PE's de la red). En tal escenario se necesitaría que los enrutadores de distribución (PE's) fuesen ahora doble pila (soporte de IPv4 hacia el core MPLS e IPv6 a nivel WAN y para la configuración de los túneles respectivos) y los enrutadores de acceso sólo necesitarían soportar IPv6 además de configurar un protocolo de ruteo IPv6 a nivel de LAN y WAN.

De forma similar a la propuesta de implementación de túneles manuales (manual y GRE) en los enrutadores de distribución, se puede mejorar la funcionalidad de las soluciones con túneles dinámicos (6to4 e IPv6 compatible IPv4) al reducir el número de túneles a configurar a 1 por cada PE en la red, sin importar el número de islas IPv6 a interconectar. En el caso de utilizar ruteo dinámico se reduce además de la misma manera el número de sistemas autónomos a configurar para la redistribución de rutas IPv6.

Los métodos de interconexión realizadas anteriormente tienen cabida cuando no se soporta 6PE ni 6VPE en los enrutadores de distribución (PE's) o bien se necesita una rápida y fácil implementación (en contraste con 6PE y 6VPE, los cuales requieren de mayores exigencias en cuanto a configuración).

6. AGRADECIMIENTOS

Un especial agradecimiento a los estudiantes de Ingeniería de Sistemas y Electrónica de la Universidad Distrital Francisco José de Caldas y al Ingeniero Pablo López.

Referencias Bibliográficas

[1] S. Deering, R. Hinden; Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, 1995.

[2] M. Tatipamula, P. Grossetete, P. H. Esaki; IPv6 integration and coexistence strategies for next-generation networks, Communications Magazine, IEEE. Volume 42 Issue 1, pp 88-96, 2004.

[3] Cisco IOS IPv6; Configuration guide, release 12.4 implementing tunneling for IPv6. [En línea], consultado en Febrero 10 de 2010, disponible en: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-tunnel.html.

[4] D. López, C. Hernández, O. Salcedo; Propuesta de interconexión mediante técnicas de entunelamiento de islas IPv6 a través de una infraestructura de core MPLS/IPv4 con enrutadores de distribución de doble pila, Revista Tecnura, Vol. 16, no 32, pp 50-58, 2012.

[5] A. Polyrakis, D. Kalogeras; 6PE: IPv6 over MPLS, Cisco Exposition January 2005. [En línea], consultado en Enero 9 de 2010, disponible en: http://www.netmode.ntua.gr/Presentations/6PE%20-%20IPv6%20over%20MPLS%20(cisco%20expo%2005).pdf.

[6] P. Grossetete; IPv6 over MPLS Cisco IPv6 provider edge router (6PE) Cisco IPv6 VPN provider edge router (6VPE). [En línea], consultado en Junio 20 de 2010, disponible en: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/prod_presentation0900aecd80311df4.pdf.

[7] Huawei Technologies Co ; Golden Bridge to the Next-Generation Internet, Brief Analysis of IPv6 Transition Technologies. [En línea], consultado en Febrero 19 de 2011, disponible en: http://www.huawei.com/products/datacomm/detailitem/view.do?id=3066&rid=1555

[8] F. Tremplin, T. Gleeson, M. Talwar, D. Thaler; Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), RFC 4214, 2005.

[9] E. Nordmark, R. Gilligan; Transition mechanisms for IPv6 hosts and enrutadores, RFC 2893, 2000.

[10] D. Farinacci, T. Li, et al ; Generic Routing Encapsulation (GRE), RFC 2784 (proposed standard - updated by RFC

2890), 2000.
[11] B. Carpenter, K. Moore, K; Connection of IPv6 domains via IPv4 clouds, RFC 3056, 2001.
[12] R. Hinden, S. Deering; IP version 6 addressing architecture, RFC 4291, 2006.
[13] I. Beijnum; Running IPv6, Editorial Apress, Chapter 3, pp 34, 2006.
[14] Cisco Files, Interconnecting ipv6 domains using tunnels, consultado en Marzo 19 de 2010, disponible en: http://www.ipv6-tf.com.pt/implementacoes/files/cisco/ipv6_.erconnectingIPv6DomainsUsingTunnels.pdf
[15] P. Marques, F. Dupont; Use of BGP-4 multiprotocol extensions for IPv6 inter-domain routing, RFC 2545, 1999.
[16] L. Qing, T. Jinmei, K. Shima; ipv6 advanced protocols implementation, Editorial Morgan Kaufmann, Chapter 1, pp 17-32 2007.
[17] Voip-Info.org ; VoIP QoS requirements. [En línea], consultado en Febrero 8 de 2010, disponible en: http://www.voip-info.org/wiki/view/QoS.
[18] VoIP Troubleshooter LLC; Indepth: Jitter. [En línea], consultado en Enrero 15 de 2010, disponible en: http://www.voiptroubleshooter.com/indepth/jittersources.html.
[19] A. García;. Estudio de la inclusión del sistema PCE en redes GMPLS. [En línea], consultado en Marzo 10 de 2010, disponible en: upcommons.upc.edu/pfc/bitstream/2099.1/8773/1/Proyecto%20PCE.pdf.