

# Implementación del servicio de videoconferencia sobre una infraestructura IPv6 con los protocolos PIM y OSPFv3

*Implementation of videoconferencing on a IPv6 infrastructure with the PIM and OSPFv3 protocols*

Samuel E. González

Hospital Universitario Clínica San Rafael  
saedgo@gmail.com

Helbert Guzmán Vásquez

Wawa CEA  
administrador@wawa.com.co

Guillermo A. Hurtado

Universidad Distrital Francisco José de Caldas  
gahurtador@udistrital.edu.co

Partiendo de la necesidad de dominar las tecnologías de punta y las tendencias en cuanto a desarrollo tecnológico, surge la idea de planificar y diseñar un prototipo de lo que fue una infraestructura tecnológica para la emisión de video como lo son las videoconferencias; con tecnología Cisco y protocolos de enrutamiento como OSPFv3 y PIM, con ello se busca dar las mejores pautas a la hora de implementar este servicio sobre la IPv6 la cual cada vez va a ser más adoptada por la mayoría del mundo debido al agotamiento inminente de las direcciones IPv4, mostrando de alguna manera las ventajas que trae la implementación del servicio sobre IPv6 y como son aprovechadas sus características para la administración de dicho servicio.

*Palabras clave:* IPv6, OSPFv3, PIM, top down, videoconferencia

Based on the need to master the latest technologies and trends in technology development the idea of planning and designing a prototype of what may be a technological infrastructure for the broadcast video such as video conferencing, to Cisco technology and protocols as OSPFv3 routing and PIM, thus we give the best guidance when implementing this service on the IPv6 which ever going to be more taken by the majority of the world due to the imminent exhaustion of IPv4 addresses, showing some way the benefits that brings service deployment on IPv6 and how they are exploited its features for managing the service.

*Keywords:* IPv6, OSPFv3, PIM, top down, videoconference

## Introducción

La implementación y ejecución del servicio de videoconferencia (compresión digital de audio y video en tiempo real) empleando el códec de la tarjeta de red de los PC se ejecuta actualmente sin problema en la infraestructura IPv4. Puesto que todos los dispositivos se encuentran configurados con los 32 bits de direccionamiento IP. Lastimosamente las combinaciones de los cuatro grupos de octetos de bits que conforman la IPv4 se están acabando, dando paso a la nueva versión del protocolo IP que ofrece una combinación de 128 bits, muchísimo más amplia que su versión anterior, recibiendo el nombre de IPv6 (Raicu y Zeadally, 2003; Tatipamula, Grossetete, y Esaki, 2004; Wiljakka, 2002).

En muchos aspectos IPv6 es una extensión conservadora de IPv4, de hecho especifica un nuevo formato de paquete,

---

Fecha recepción del manuscrito: Octubre 17, 2012

Fecha aceptación del manuscrito: Diciembre 10, 2012

Samuel E. González, Hospital Universitario Clínica San Rafael; Helbert Guzmán Vásquez, Wawa CEA; Guillermo A. Hurtado, Facultad Tecnológica, Universidad Distrital Francisco José de Caldas.

Esta investigación fue financiada por: Universidad Distrital Francisco José de Caldas.

Correspondencia en relación con el artículo debe ser enviada a: Helbert Guzmán Vásquez. Email: administrador@wawa.com.co

diseñado para minimizar el procesamiento del encabezado de tramas. Dado que las cabeceras de los paquetes IPv4 e IPv6 son significativamente distintas, los dos protocolos no son interoperables.

Por lo general las direcciones IPv6 están compuestas por dos partes lógicas, un prefijo de 64 bits y otra parte de 64 bits que corresponde al identificador de interfaz, que casi siempre se genera automáticamente a partir de la dirección MAC (*Media Access Control address*) de la interfaz a la que está asignada la dirección. Esta dirección es un número hexadecimal fijo que es asignado a la tarjeta o dispositivo de red del fabricante por la dirección IP, dado que la dirección IP se puede cambiar.

La utilización de IPv6 se ha frenado por la traducción de direcciones de red NAT (*Network Address Translation*). Temporalmente se ha aliviado la falta de estas direcciones de red mediante un mecanismo que consiste en usar una dirección IPv4 para que una red completa pueda acceder a internet. Pero esta solución impide la utilización de varias aplicaciones, ya que sus protocolos no son capaces de atravesar los dispositivos NAT, por ejemplo P2P, voz sobre IP (VoIP), juegos multiusuarios, entre otros (Bacca, Noguera, Baldiris, Guevara, y Fabregat, 2011). Como en la actualidad aun no se tiene en cuenta la configuración IPv6 por soluciones como los dispositivos NAT o los túneles IPv4/IPv6, no se ha podido acceder totalmente a un ambiente IPv6.

Con IPv4 debido a sus características, como que en su cabecera de paquete no usa etiquetas de contenido, no se permite optimizar el rendimiento de algunos servicios, como el de videoconferencia, debido a que al no etiquetar el paquete según tipo de dato se niega la posibilidad de priorizar directamente el servicio, cargando a los enrutadores de mas procesamiento de datos, dando como resultado saltos y algunas veces interrupciones en su transmisión. OSPF versión 2 tiene algunas similitudes con OSPF versión 3, como tipos básicos de paquetes, algoritmos para el descubrimiento de vecinos y calculo de adyacencias, tipos de interfaces como p2p, y tratamiento de LSAs. Sin embargo no soporta IPv6 entre otras características, impidiendo enrutar cualquier tipo de servicio en el protocolo versión 6, lo que obliga a usar un protocolo que tenga este tipo de características y que soporte la nueva versión de IP en este caso la IPv6.

Pim como protocolo de *multicast* sigue siendo útil y funciona de manera transparente entre versiones, aunque su señalización entre *routers* y *host* varía según la versión IP que se use.

IPv6 posee una infraestructura de direcciones y enrutamiento eficaz y jerárquica. A partir de allí, se puede comprobar cuál sería la mejora de compatibilidad para Calidad de Servicio (QoS) y Clase de Servicio (CoS), y la seguridad Integrada (IPsec), que permite autenticación

y encriptación del propio protocolo base, de forma que todas las aplicaciones se puedan beneficiar de ello, y el envío de un mismo paquete a un grupo de receptores. Todo esto es posible de constatar por medio de la ejecución de un proyecto palpable y tangible, en donde se implemente un servicio de red en infraestructura en donde solo se evidencie la IPv6. Con este proyecto es posible evaluar el comportamiento de IPv6, elaborado una propuesta tecnológica que beneficie y sea soporte para los conflictos que existen en las aplicaciones web implementadas en IPv6, y con ello establecer parámetros y recomendaciones primordiales al momento de implementar un servicio sobre IPv6 con una tecnología de comunicaciones específica.

Por lo anterior, en este proyecto se emplean herramientas de emulación bajo la tecnología CISCO y software libre, que permiten dar pautas, establecer parámetros y recomendaciones para implementar el servicio de videoconferencia en una infraestructura IPv6 bajo los protocolos PIM y OSPFv3. El rendimiento y calidad del servicio implementado en la red emulada, arroja una mejora del servicio de videoconferencia en IPv6 frente al el mismo implementado en IPv4. Al no tener dispositivos de IPv6 y en consecuencia, aplicaciones que solo pueden ser evidenciadas por IPv4, se ha podido dar a conocer el camino a seguir para poder realizar comunicaciones sobre una infraestructura IPv6 mostrando el servicio de videoconferencia

## Metodología

### Planeación, diseño, implementación, funcionamiento y optimización (PDIOO)

Las fases del ciclo de vida de una red hacen referencia a la documentación de CISCO, en las cuales se realizaran las siguientes actividades.

*Planeación.* En esta fase los requisitos de red se identifican, también incluye un previo análisis de las áreas donde se va a instalar la red, al igual que una identificación de los usuarios que requieren servicios de red (Anderson, 1992). En esta fase el principal objetivo es entender las soluciones que presentan los usuarios de la videoconferencia IPv6 y el impacto que la infraestructura de comunicaciones y/o los servicios que se desean habilitar, tendrían sobre su productividad y estructura de costos. Se identifican los requerimientos, puntualmente en este caso la videoconferencia IPv6 con protocolos PIM y OSFPv3, así como las métricas a considerar para el éxito del proyecto. Igualmente, se analiza la infraestructura tecnológica existente para luego determinar su uso y evolución dentro de los planes existentes.

*Diseño.* En esta fase, los diseñadores de redes realizaron la mayor parte de la lógica y el diseño físico, según los requisitos recogidos durante la fase de planeación.

**Implementación.** Después de que el proyecto se aprobó, la aplicación comienza. La red se construye de acuerdo a las especificaciones de diseño. La aplicación también sirve para verificar el diseño.

**Funcionamiento.** La operación es la última prueba de la eficacia del diseño de la red en la cual se monitorea. Durante esta fase para los problemas de rendimiento y fallos para proporcionar cualquier de entrada en la fase de optimización del ciclo de vida de la red.

**Optimización.** La fase de optimización se basa en la gestión proactiva de la red que identifica y resuelve los problemas antes de las interrupciones de la red surgen. La fase de optimización puede conducir a un re-diseño de la red si demasiados problemas surgen debido a errores de diseño o como se degrada el rendimiento de la red a través del tiempo como el uso real y capacidades divergentes. Re-diseño también puede ser necesario cuando las necesidades cambian significativamente.

### **Requisitos de la infraestructura para soportar IPv6 (Gilligan, Nordmark, y IETF-ngtrans-mech . Txt, 2000)**

**Requerimientos para host (Hamarsheh y Goossens, 2011).** *Soprote Obligatorio:* Especificación básica de IPv6 [RFC2460], Arquitectura de direccionamiento básico en IPv6 [RFC4291], selección de dirección por defecto [RFC3484], ICMPv6 [RFC4443], cliente DHCPv6 [RFC3315], SLAAC [RFC4862], path MTU Discovery [RFC1981], Neighbour Discovery [RFC4861], mecanismos básicos de transición para hosts IPv6 y routers [RFC4213], IPsec-v2 [RFC2401, RFC2406, RFC2402], IKE version 2 (IKEv2) [RFC4306, RFC4718], si se requiere soporte de movilidad sobre IPv6, el dispositivo debe cumplir con MIPv6 [RFC3775] y Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture [RFC4877], extensiones del protocolo DNS para incorporar extensiones de registros DNS IPv6 [RFC3596], mecanismo DNS de extensión de mensaje (NAP Colombia, 2011).

**Requerimientos para equipamiento switches capa 2 de nivel.** *PyME Soprote Obligatorio:* MLDv2 snooping [RFC4541], soporte opcional (administración), especificación básica de IPv6 [RFC2460], arquitectura de direccionamiento básico en IPv6 [RFC4291], selección de dirección por defecto [RFC3484], ICMPv6 [RFC4443], SLAAC [RFC4862], protocolo SNMP [RFC3411], soporte SNMP, [RFC3412, RFC3413, RFC3414], MLDv2 snooping [RFC4541], DHCPv6 snooping [RFC3315], mensajes DHCPv6 deben ser bloqueados entre suscriptores y la red de modo a que falsos servidores DHCPv6 no puedan distribuir direcciones, filtrado del Router Advertisement (RA) [RFC2462, RFC5006], filtrado del RA debe ser utilizado en la red de modo a bloquear mensajes RA no autorizados, inspección dinámica de IPv6 neighbour solicitation/advertisement [RFC2461].

**Requerimientos para routers capa 3.** Especificación básica de IPv6 [RFC2460], arquitectura de direccionamiento básico en IPv6 [RFC4291], selección de dirección por defecto [RFC3484], ICMPv6 [RFC4443], SLAAC [RFC4862], MLDv2 snooping [RFC4541], opción Router-Alert [RFC2711], path MTU Discovery [RFC1981], neighbour Discovery [RFC4861], classless inter-domain routing [RFC4632].

Si se requiere protocolo IGP, entonces se requiere soporte para RIPng [RFC2080], OSPF-v3 [RFC5340] o IS-IS [RFC5308]. Si se requiere soporte OSPF-v3, el equipo de cumplir con Authentication/Confidentiality for OSPF-v3 [RFC4552]. Si se requiere soporte para el protocolo BGP4, el equipo debe cumplir con RFC4271, RFC1772, RFC4760, RFC1997, RFC3392 y RFC2545, soporte para QoS [RFC2474, RFC3140], mecanismos básicos de transición para hosts IPv6 y Routers [RFC4213], utilización de IPsec para la creación segura de túneles IPv6-in-IPv4 [RFC4891], Generic Packet Tunneling e IPv6(11) [RFC2473]. Si se requiere 6PE, el equipo debe cumplir con Connecting IPv6 Island over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE) [RFC4798], Multicast Listener Discovery versión 2 [RFC3810]. Si se requiere soporte de Movilidad sobre IPv6, el dispositivo debe cumplir con MIPv6 [RFC3775] y Mobile IPv6 Operation With IKEv2.

### **Multicast PIM**

Es un protocolo de encaminamiento *multicast*, en el cual, por medio de tablas de rutas del protocolo de encaminamiento *unicast* subyacente, se construyen los árboles de distribución *multicast*. En este protocolo se encuentran dos tipos de funcionamiento, modo denso y modo disperso.

**Modo denso.** Consiste en que los miembros de una red se suscriban a un determinado grupo *multicast*, obligando a operar la totalidad de los *routers* a ejecutar entidades del protocolo PIM.

**Modo disperso.** Este consiste de un número de *routers* que tienen asociados miembros de grupos *multicast* pequeño en comparación con el total de *routers* de la red, y los miembros del grupo están además dispersos por toda la red.

Por otro lado PIM SM permite usar árboles SPT (*Shortest Path Tree*, árboles basados en el camino más corto), por medio de la unión directa de un miembro *multicast* a una fuente en concreto, reduciendo los retardos asociados a los árboles compartidos, aumentando la información de estado *multicast* que ha de ser mantenida por las entidades *multicast* que operan en los *routers*.

### **Protocolo OSPFv3**

Este es un protocolo de enrutamiento jerárquico. Emplea el algoritmo Dijkstra enlace-estado (LSA - *Link State Algorithm*), calculando la ruta más corta. OSPF se puede

descomponer en regiones (áreas). Hay un área especial llamada área *backbone*, formando la parte central de la red de donde las otras áreas de la red se conectan con ella. Con esto, el protocolo de enrutamiento se extiende para apoyar difusión ilimitada, después de analizar la similitud y la diferencia entre la difusión ilimitada y *unicast*. También se implementó AOSPF y se probó con éxito en nuestro banco de pruebas de IPv6. El análisis de rendimiento muestra una baja sobrecarga de AOSPF.

**Resultados**

La Fig. 1 muestra el montaje de la red para servicio de video conferencia.

Donde:

- Área 0 zona de backbone
- Área 1 zona de LAN Bogotá
- Área 2 zona de LAN Cali
- Área 3 zona de LAN Barranquilla
- Área 4 zona de LAN Medellín

En el caso del *router* de Bogotá (Fig. 2 y tabla 1) se tiene que:

- Área 1: Área OSPF designada para LAN en *router* Bogotá.
- RBOG: Nick designado al *router* Bogotá.
- Área 0: Área OSPF designada para *backbone* en *router* Bogotá.
- FE: Interface *Fast Ethernet*.

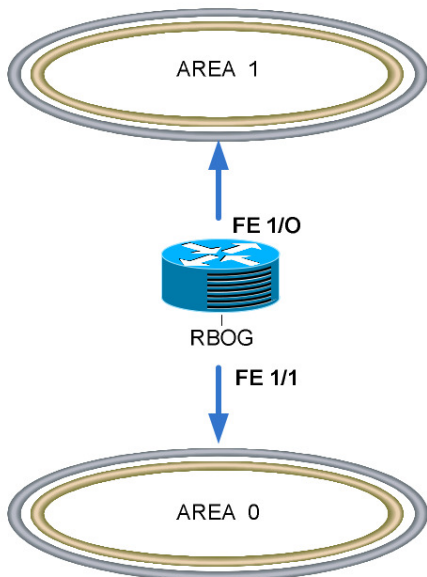


Figura 2. Topología de red router Bogotá.

- En el caso del *router* de Cali (Fig. 3 y tabla 2) se tiene que:
- Área 2: Área OSPF designada para LAN en *router* Cali.
  - RCAL: Nick designado al *router* Cali.
  - Área 0: Área OSPF designada para *backbone* en *router* Cali.

Tabla 1  
Router Bogotá.

Router BOG				
	IPV 4	subnetmask	IPV 6	Subnetmask
FA 1/1	192.168.1.1	24	fe80::c0a8:101	128
FA 1/0	10.10.1.13	30	fe80::a0a:101	126

- FE: Interface *Fast Ethernet*.

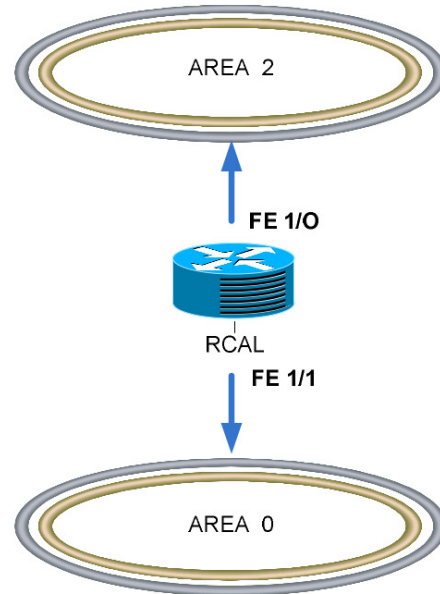


Figura 3. Topología de red router Cali.

Tabla 2  
Router Cali.

Router CAL				
	IPV 4	subnetmask	IPV 6	Subnetmask
FA 1/1	192.168.2.1	24	fe80::c0a8:201	120
FA 1/0	10.10.1.9	30	fe80::a0a:109	126

En el caso del *router* de Medellín (Fig. 4 y tabla 3) se tiene que:

- Área 3: Área OSPF designada para LAN en *router* Medellín.
- RMED: Nick designado al *router* Medellín.
- Área 0: Área OSPF designada para *backbone* en *router* Medellín.
- FE: Interface *Fast Ethernet*.

Tabla 3  
Router Medellín.

Router MED				
	IPV 4	Subnetmask	IPV 6	Subnetmask
FA 1/1	192.168.3.1	24	fe80::c0a8:301	120
FA 1/0	10.10.1.5	30	fe80::a0a:105	126

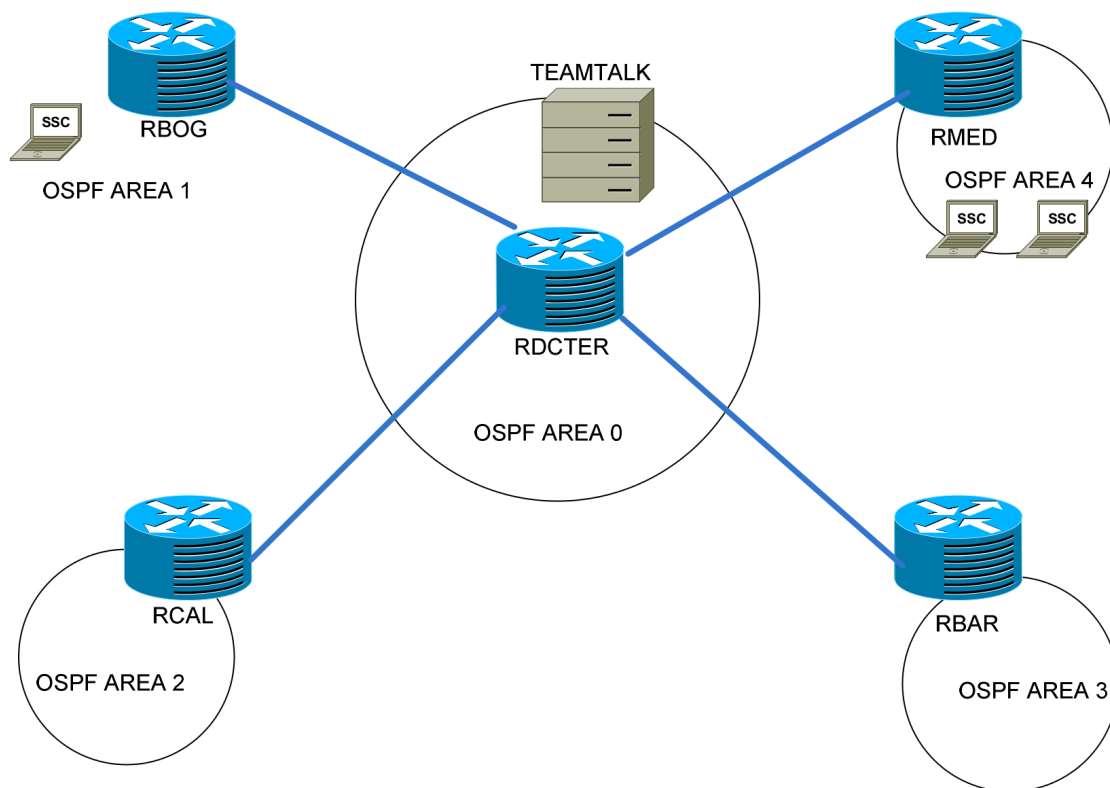


Figura 1. Diagrama OSPF con sus respectivas áreas.

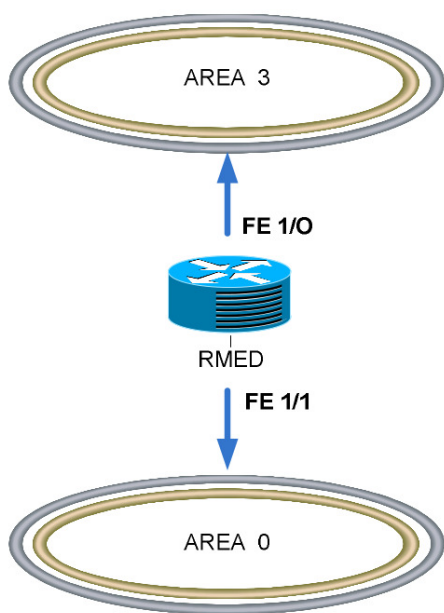


Figura 4. Topología de red router Medellín.

En el caso del *router* de Barranquilla (Fig. 5 y tabla 4) se tiene que:

- Área 4: Área OSPF designada para LAN en *router* Barranquilla.
- RBAR: Nick designado al *router* Barranquilla.
- Área 0: Área OSPF designada para *backbone* en *router* Barranquilla.
- FE: Interface *Fast Ethernet*.

Tabla 4  
Router Barranquilla.

Router BAR				
	IPV 4	subnetmask	IPV 6	subnetmask
FA 1/1	192.168.4.1	24	fe80::c0a8:401	120
FA 1/0	10.10.1.1	30	fe80::a0a:101	126

En el caso del *router* del Datacenter (Fig. 6 y tabla 5) se tiene que:

- RDCENTER: Nick designado al *router* Datacenter.
- Área 0: Área OSPF designada para *backbone* en *router* RDCENTER.
- FE: Interface *Fast Ethernet*.

### Resultados esperados

Se espera que al realizar la implementación de la infraestructura IPv6 *multicast* sobre Pim y OSPFv3, para el servicio de videoconferencia, se puedan tener pautas para



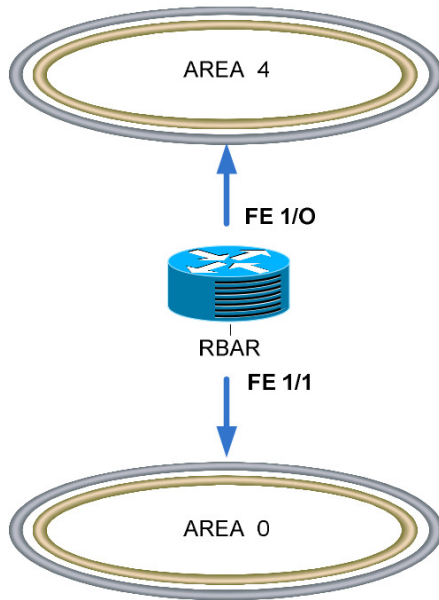


Figura 5. Topología de red router Barranquilla.

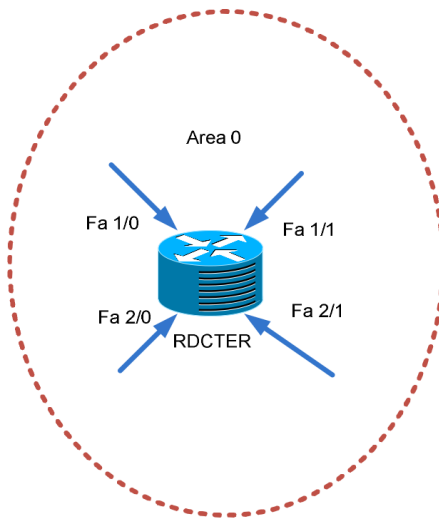


Figura 6. Topología de red router DATACENTER.

Tabla 5  
Router Datacenter.

Router DCENTER				
FA1/0	10.10.1.14	30	fe80::a0a:10e	126
FA1/1	10.10.1.10	30	fe80::a0a:10a	126
FA2/0	10.10.1.6	30	fe80::a0a:106	126
FA2/1	10.10.1.1	30	fe80::a0a:101	126

la resolución del problema de asimilación del protocolo en la nueva tendencia de las comunicaciones, en nuestro caso particular de la comunicación simultánea bidireccional de audio y vídeo en tiempo real.

Se busca simular en la nube IPv6 operando a nivel de dominios cerrados e inter-dominio, pudiendo ser usado en principio como único protocolo para el establecimiento de un estado de encaminamiento *multicast* a través de un escenario completo inter-dominio, un servidor de videoconferencias con OSPF y Pim.

Se pretende identificar los factores que inciden negativamente en el proceso de actualización a IPv6 como el despliegue y puesta en funcionamiento del protocolo el cual necesita el soporte tanto de los *routers* en el interior de cada dominio como de los existentes en las fronteras entre dominios de red.

### Conclusiones

Se debe identificar los factores que inciden negativamente en el proceso de actualización a IPv6. Los procedimientos y recomendaciones propuestas se deben usar en la implementación del servicio de videoconferencia en IPv6. Al escoger el tipo de protocolos adecuados para este diseño de infraestructura tecnológica se pretende obtener un buen servicio.

### Referencias

Anderson, R. E. (1992). Social impacts of computing: Codes of professional ethics. *Social Science Computer Review*, 10(4), 453-469.

Bacca, J., Noguera, A., Baldiris, S., Guevara, J., y Fabregat, R. (2011). Sistema de procesamiento distribuido como soporte al módulo de búsqueda sobre repositorios de objetos virtuales de aprendizaje para la plataforma de e-learning dotlrn. *Revista Tekhnê*, 8(1), 69-73.

Gilligan, R. E., Nordmark, E., y ietf-ngtrans-mech . Txt, D. (2000). *Status of this memo transition mechanisms for ipv6 hosts and routers*.

Hamarshesh, A., y Goossens, M. (2011). *Hosts with any network connectivity using bump-in-the-ap (bia) draft-hamarshesh-behave-biav2-03*.

NAP Colombia. (2011). *Practica de configuración de routers*. Descargado de [http://www.6deploy.eu/workshops2/20101112\\_madrid\\_spain/DIA1-3-routing-Help\\_Commands\\_Cisco.pdf](http://www.6deploy.eu/workshops2/20101112_madrid_spain/DIA1-3-routing-Help_Commands_Cisco.pdf)

Raicu, I., y Zeadally, S. (2003). Evaluating ipv4 to ipv6 transition mechanisms. En *10th international conference telecommunications ict2003* (Vol. 2, p. 1091-1098).

Tatipamula, M., Grossetete, P., y Esaki, H. (2004). IPv6 integration and coexistence strategies for next-generation networks. *IEEE Communications Magazine*, 42(1), 88-96.

Wiljakka, J. (2002). Transition to ipv6 in gprs and wcdma mobile networks. *IEEE Communications Magazine*, 40(4), 134-140.