

Modelaje de protocolos de membresía de grupos IP Multicast en redes Ethernet conmutadas. Caso de estudio: utilización de la videoconferencia

Carlos M. MORENO;
Departamento de Comunicaciones, Universidad Central de Venezuela
Caracas, Distrito Metropolitano Apdo. Postal 47747 – Zona 1051

y

Luis J. FERNÁNDEZ
Departamento de Comunicaciones, Universidad Central de Venezuela
Caracas, Distrito Metropolitano Apdo. Postal 47747 – Zona 1051

RESUMEN

El presente trabajo ofrece dos aportes significativos. El primero de ellos es el empleo de una metodología basada en eventos para la creación de un modelo de simulación genérico que contempla cualquiera de los protocolos de membresía de grupos IP Multicast estudiados (IGMP Snooping, CGMP y GMRP) conjuntamente con el protocolo IGMP. El segundo aporte consiste en el uso de los elementos que provee un sistema operativo multihilos para el modelaje; ésto se puede lograr empleando conceptos de programación orientada a objetos. Tal modelo representa la existencia de tráfico de tipo isócrono (Voz y video) conjuntamente con tráfico de tipo anisócrono (Protocolos de membresía de grupos e IGMP) considerando un escenario particular, el cual consiste en un proceso de adherencia y desincorporación de un terminal a una sesión de videoconferencia sobre protocolo IP previamente establecida con el estándar UIT H.323 entre dos terminales.

Palabras Claves: Multicast, modelo, protocolos, membresía, ethernet, conmutada, videoconferencia.

1. INTRODUCCIÓN

En la actualidad, los servicios de voz, datos y video tienden a ser integrados en una misma plataforma de red, lográndose así la “Convergencia”, término muy utilizado por las empresas fabricantes de tecnología de redes. El diseño de una infraestructura de integración de servicios (voz, datos y video) debe tomar en consideración los requerimientos de las aplicaciones que serán implantadas. La videoconferencia constituye una de tales aplicaciones, y es la que demanda la mayor cantidad de recursos de la red [8], por lo que se necesita una calidad de servicio deseable para ofrecer este servicio. El protocolo IP Multicast permite establecer videoconferencias punto-multipunto, sobre una red de conmutación de paquetes, ofreciendo un ahorro sustancial en la utilización de los recursos en una red ethernet conmutada. Para ello es necesario que los equipos activos reconozcan los grupos IP multicast identificados por direcciones IP clase D, por lo que se han diseñado protocolos de membresía de grupos IP multicast (ej. IGMP Snooping, GMRP y CGMP) para redes ethernet conmutadas que funcionan en las primeras dos capas del modelo OSI. Se pretende modelar el mismo escenario planteado de adherencia y desincorporación de un terminal a una sesión de videoconferencia con la utilización de cada uno de estos

protocolos. Cada uno de ellos produce un efecto distinto sobre el rendimiento de la sesión, por lo que es conveniente establecer parámetros de estudio en cada caso tales como el jitter, el retardo, el grado de utilización de la red y la tasa de pérdida de tramas para poder establecer comparaciones. Tal modelo, conjuntamente con los parámetros de rendimiento preestablecidos, sirven de base para la realización de simulaciones en trabajos posteriores.

2. PROTOCOLO IP MULTICAST

El protocolo IP Multicast permite la transmisión de datagramas IP a un conjunto de anfitriones que forman parte de grupos de multidifusión [13]. Se emplea básicamente el mismo concepto de entrega con el mejor esfuerzo, como en el caso de los datagramas IP Unicast. Esto compromete la calidad de servicio en la realización de videoconferencias. La pertenencia a un grupo de protocolo IP Multicast es un proceso dinámico. Un anfitrión puede unirse o abandonar un grupo en cualquier momento. Cada grupo IP Multicast tiene una dirección de multidifusión única (clase D). Así como en el caso de las direcciones IPv4 Clase A,B y C algunas direcciones de multidifusión IP Clase D son asignadas por la Autoridad de Internet (IANA) y corresponden a grupos que siempre existen aun cuando actualmente no tengan miembros. Otras direcciones de multidifusión están disponibles para usos temporales y corresponden a grupos transitorios de multidifusión que se crean cuando son necesarios y se desechan cuando el número de miembros llega a 0. Los mensajes IGMP son transmitidos dentro de datagramas IP, cuyo campo de protocolo de capa superior se establece con un valor de dos, y el campo de tiempo de vida con un valor de cero. A su vez, dicho paquete IP es encapsulado en tramas ethernet, en donde la dirección MAC destino contiene los 23 bits menos significativos de la dirección de grupo añadidos, al patrón hexadecimal 0x0100.5EXX.XXXX. El protocolo IP Multicast puede utilizarse en una sola red LAN o a través de una red de redes [13]. En este último caso, enrutadores de multidifusión especiales envían los datagramas de multidifusión. Para la realización de videoconferencias punto-multipunto bajo el estándar UIT H.323 [1],[8] es posible utilizar el protocolo IP Multicast, y en el caso particular de redes LAN ethernet conmutadas en las que los equipos activos presentan funciones básicas correspondientes a las dos primeras capas del modelo OSI, existen tres protocolos de membresía de grupos IP Multicast (IGMP Snooping, GMRP y CGMP) que se pueden

utilizar para el reconocimiento de los grupos de multidifusión, trabajando conjuntamente con el protocolo IGMP. Este último se emplea tanto por parte de los miembros de grupos así como por parte de un enrutador denominado consultor, para gestionar el proceso de adherencia y desincorporación. Este proceso se realiza cuando un terminal de videoconferencia H.323 UIT manifiesta su intención de participar en una sesión previamente establecida entre dos terminales, e involucra tanto al conmutador conectado directamente, así como al enrutador consultor, ocasionando una degradación de la calidad de servicio de la sesión. Tal efecto dependerá de las características del protocolo de membresía de grupo utilizado.

3. PROTOCOLO DE GESTIÓN DE GRUPOS INTERNET (IGMP)

IGMP v1 (Versión 1)

La primera versión del protocolo IGMP define procesos de consulta-respuesta, adherencia, desincorporación a grupos y un mecanismo de supresión de reporte [12].

Proceso de consulta-respuesta y mecanismo de supresión: permite al enrutador consultor determinar cuáles grupos de multidifusión están activos, es decir, si hay uno o más miembros interesados en la subred. El enrutador consultor envía cada 60 segundos un mensaje de consulta a los grupos presentes en una subred. De cada uno de ellos, un anfitrión miembro responde con un mensaje de reporte, representando al grupo, luego que expira un contador propio inicializado en 10 segundos por defecto. Se asocia entonces un contador distinto por cada grupo al cual pertenece, y es posible que dicho anfitrión no represente a los otros grupos a los que pertenece necesariamente. De esta forma, el enrutador consultor mantiene una tabla de los grupos existentes en la subred consultada y específicamente de los terminales H.323 UIT participantes en una sesión de videoconferencia punto-multipunto.

Proceso de adherencia y desincorporación: si un anfitrión desea formar parte de algún grupo, puede enviar un mensaje de adherencia no solicitada de reporte al mismo. De esta forma, el anfitrión puede enviar y recibir información al grupo. Si se realiza una sesión de videoconferencia entre dos terminales H.323 UIT, un terminal adicional puede manifestar su intención de participar. Lamentablemente, si un anfitrión desea desincorporarse de algún grupo de multidifusión no tiene forma de manifestar intencionalmente su intención si utiliza la primera versión del protocolo IGMP. El anfitrión sólo debe dejar de enviar mensajes de reporte al enrutador consultor de la subred, para dejar de recibir información al grupo. Como resultado de esto, un terminal H.323 UIT dejaría de recibir tráfico de la sesión de videoconferencia. El tiempo que tarda el enrutador en desincorporar al anfitrión de la sesión, es de 3 minutos, por lo que el terminal H.323 UIT todavía recibe tráfico multimedia en ese intervalo de tiempo, teniendo como consecuencia una degradación de la calidad de servicio por congestión si inmediatamente desea formar parte de otra sesión, ya que habría un aumento en el grado de utilización de la red.

IGMPv2 (Versión 2)

Los mensajes de consulta y de reporte en IGMPv2 son idénticos a los de IGMPv1 con 2 excepciones: la primera es que los mensajes de consulta se dividen en dos subtipos: generales y específicos [11]. Los mensajes generales de consulta realizan las mismas funciones en ambas versiones. Los mensajes específicos de consulta, van dirigidos a grupos particulares.

La segunda excepción es que los mensajes de reporte tienen diferentes tipos de código. Un nuevo campo en los mensajes de consulta permiten al enrutador consultor especificar el máximo tiempo de consulta-respuesta para disminuir la latencia de desincorporación de anfitriones a grupos. En una sesión de videoconferencia, la disminución conlleva a un decremento en la latencia de salida.

Otra de las diferencias con respecto a IGMPv1, es que en IGMPv2 el anfitrión puede enviar al enrutador consultor de la subred un mensaje de desincorporación, produciendo igualmente una disminución en la latencia de salida. Al disminuir el máximo tiempo de respuesta a la consulta (Límite superior de contador individual), aumentan las ráfagas, y los picos de congestión, degradando fuertemente la calidad de servicio; de lo contrario, si se aumenta, se incrementa la latencia de salida.

Debido a que IGMPv2 define que no necesariamente deben haber mensajes de desincorporación de grupos específicos, es posible que los conmutadores ethernet no identifiquen tal desincorporación, utilizando de forma equivocada algunos protocolos de membresía de grupos de red LAN conmutada.

IGMP v3 (Versión 3)

La versión 3 del protocolo IGMP amplía los mecanismos de adherencia y desincorporación de anfitriones[10]. Permite a los miembros de un grupo seleccionar las fuentes de tráfico específicas de las cuales desean recibir tráfico aún dentro del mismo grupo.

Se presentan mensajes de consulta y de reporte. Los mensajes de consulta pueden ser: generales, de grupo específico y de grupo-fuente específico. Los primeros son enviados por el enrutador en la subred para aprender acerca del estado de recepción de las interfaces. Los segundos son enviados para verificar el estado de recepción de un grupo específico. Los mensajes de grupo-fuente específicos son enviados por el consultor para verificar si alguno de los anfitriones vecinos desea recibir paquetes enviados a un grupo particular por parte de un conjunto de fuentes. Esto permitiría a un terminal H.323 UIT en una sesión de videoconferencia punto-multipunto, seleccionar los terminales de los cuales desea recibir tráfico de video y audio entre los integrantes de dicha sesión.

4. PROTOCOLOS DE MEMBRESÍA IP MULTICAST PARA RED LAN CONMUTADA

IGMP Snooping

Se requiere que el conmutador ethernet lea los mensajes IGMP que se transmiten entre un anfitrión y el enrutador. Cuando el conmutador escucha un reporte de adherencia IGMP de un anfitrión para un grupo de multidifusión particular, se añade el número de puerto del anfitrión a la entrada asociada en la tabla CAM (Memoria de acceso direccionable). Si por el contrario, escucha un mensaje de salida de grupo por parte de un anfitrión, se remueve el número de puerto del anfitrión de la entrada de la tabla CAM. Dependiendo de la arquitectura del conmutador, su implementación puede ser difícil para el uso con aplicaciones multimedia sin degradar seriamente el rendimiento.

Escenario para modelaje: considérese en la Figura 1 un caso en el que el Anfitrión 1 decide formar parte del grupo 224.1.2.3 y le envía un Reporte No Solicitado de adherencia IGMP con dirección destino MAC 0x0100.5E01.0203. Esto para participar en la videoconferencia previamente establecida

entre los Anfitriones 2 y 3. Inicialmente sólo se definen entradas para los puertos 0,1,3 y 4 en la tabla CAM. Cuando el CPU (Unidad Central de procesamiento) recibe el reporte no solicitado de adherencia IGMP por parte del Anfitrión 1, se usa dicha información para llenar la tabla CAM. Como resultado, cualquier trama enviada a la dirección MAC 0x0100.5E01.0203 será reenviada a los puertos 0,1,2, 3 y 4 del conmutador.

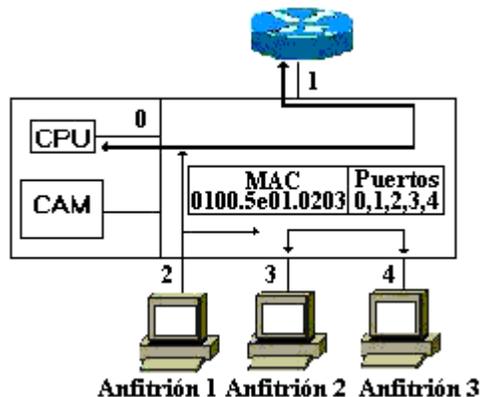


Figura 1. Añadiendo un anfitrión con IGMP Snooping

Si el Anfitrión 1 ya no desea formar parte del grupo 224.1.2.3, envía un mensaje de desincorporación no solicitado de grupo a la dirección IP 224.0.0.2 con MAC 0x0100.5E00.00.02 (si se emplean IGMPv2 o IGMPv3). Este mensaje es leído por el CPU, pero no es reenviado a través de ningún puerto. Luego el CPU del conmutador responde con otro mensaje de consulta de grupo general, de vuelta al puerto 2 para verificar si no hay más miembros del grupo 224.1.2.3 en ese puerto. Si el CPU escucha otro mensaje de Reporte IGMP de algún anfitrión por el mismo puerto, descarta el mensaje de desincorporación de grupo original y no elimina la entrada asociada al puerto 2. Si de lo contrario, no se escuchan reportes adicionales a través de dicho puerto, se elimina la entrada correspondiente en la tabla CAM.

GMRP

El protocolo genérico de registro multicast GARP conocido como GMRP permite a los conmutadores ethernet y a las estaciones anfitrionas declarar y/o eliminar dinámicamente información de miembros de grupos IP Multicast que se conectan al mismo dominio lógico, haciendo que ésta sea repartida, siempre y cuando los conmutadores soporten servicios de filtrado extendidos. Si esto es posible, se pueden registrar direcciones MAC de grupos (atributos) y asociarse a puertos físicos. Como caso particular de protocolo GARP, GMRP define una aplicación, los participantes y las declaraciones de atributos. Permite que un anfitrión envíe tramas dirigidas a los miembros respectivos de un grupo, y que cualquier conmutador por el que pasan modifiquen su comportamiento para lograrlo. Si aparece información nueva de filtraje o reconocimiento de grupos IP Multicast en un conmutador, ésta será propagada usando el protocolo GARP a través de la red, de tal forma que sean actualizadas las entradas de registro de grupos en la base de datos de filtraje de los conmutadores, formándose árboles. El funcionamiento es similar al utilizado por los enrutadores para la administración de los árboles IP Multicast en una red WAN.

Se definen tres clases de participantes: un aplicante, que hace declaraciones y puede verificar las declaraciones de otros,

puede ser una fuente o receptor multicast. Un solamente-aplicante, que pudiera ser una fuente de trabajo multicast, y un registrador, que registra declaraciones hechas por aplicantes o sólo-aplicantes.

Los mensajes GMRP, poseen varios campos, de los cuales el atributo de evento indica si es un mensaje de adherencia a grupo, o de desincorporación del mismo, lo que provocaría una declaración y un registro o una anulación de registro respectivamente.

Escenario para modelaje: considérese la presencia de un conmutador ethernet, y dos terminales H.323 UIT presentes en una sesión de videoconferencia. Ambos terminales, para formar parte del mismo grupo tuvieron que emitir un mensaje de declaración GMRP al conmutador ethernet con el mismo atributo (Dirección MAC de grupo) previamente, para que dicho conmutador haga el registro respectivo.

Un tercer anfitrión (Aplicante) desea participar en la sesión, por lo que manifiesta (Declara) su intención de participar enviando un mensaje GMRP al conmutador (Registrador), que a su vez envía un mensaje GMRP al terminal fuente de la sesión (Registrador), por lo que se une al grupo (Registro). En este proceso se añade una entrada en la tabla CAM con los puertos físicos asociados al grupo direccionado. Se realiza entonces la videoconferencia multipunto en donde dos terminales receptores H.323 UIT reciben tráfico de otro terminal fuente. Una vez que el tercer anfitrión decide salirse de la sesión, envía un mensaje de eliminación al conmutador, el cual a su vez envía otro mensaje de eliminación de registro al terminal fuente.

CGMP

Los mensajes del protocolo CGMP son encapsulados en unidades de datos de protocolo pertenecientes a la capa 2 del modelo OSI [13]. Todos los conmutadores que trabajan con este protocolo, reciben a través de sus puertos mensajes provenientes de los enrutadores, los cuales poseen un campo de código y dos campos de direccionamiento, GDA y USA cada uno con 48 bits de longitud, que identifican a un grupo destino y a un anfitrión fuente respectivamente. El campo de código se define de acuerdo a la intención del anfitrión fuente con dirección MAC contenida en el campo USA de formar parte o desincorporarse del grupo destino con dirección MAC contenida en el campo GDA. De acuerdo al campo de código de mensaje, se presentan seis tipos de mensajes: dos de adherencia y desincorporación a grupos, dos de adherencia y desincorporación de puertos en enrutador, y dos para funciones especiales de mantenimiento. La información en el campo USA se utiliza para que el conmutador asocie el número de puerto receptor al anfitrión fuente respectivo en la entrada para tráfico unicast. Usando la información en los campos de código y GDA contenida en los mensajes CGMP, el conmutador añade o elimina el número de puerto correspondiente de la entrada en la tabla CAM asociado a un grupo de multidifusión.

Escenario para modelaje: se plantea un escenario en el que un anfitrión se une a una sesión de videoconferencia previamente establecida entre dos terminales H.323 UIT (Figura 2). Se difunde un mensaje de reporte de adherencia IGMP no solicitado al grupo destino (por ejemplo 224.1.2.3) por parte del Anfitrión 1 para participar en la sesión. Este reporte IGMP pasa a través del conmutador hacia el enrutador que a su vez debe habilitar el protocolo CGMP en esa interfaz, y traducir el reporte IGMP a otro de adherencia CGMP.



Figura 2 Añadiendo un anfitrión con CGMP

El enrutador copia la dirección MAC de grupo destino (por ejemplo, 0x0100.5e01.0203) desde el mensaje de reporte IGMP al campo GDA del mensaje de adherencia CGMP. También copia la dirección MAC fuente (0x0080.c7a2.1093, por ejemplo) que es una dirección MAC de anfitrión del reporte IGMP, al campo USA del mensaje de adherencia CGMP. Una vez que ha sido creado el mensaje CGMP, se envía al conmutador. Luego éste busca una entrada en la tabla CAM para el grupo especificado en el campo GDA del mensaje. Si no se encuentra una entrada en la tabla CAM para el grupo, se crea dicha entrada añadiendo todos los puertos de enrutador a dicha lista para que todos los que están conectados al conmutador puedan recibir mensajes multicast dirigidos al grupo. Cuando un anfitrión desea desincorporarse de la sesión de videoconferencia con un mensaje IGMPv2 o IGMPv3, envía un mensaje no solicitado de desincorporación a la dirección 224.0.0.2 (Todos los enrutadores), incluyendo al enrutador consultor. Este enrutador puede simplemente traducir este mensaje de desincorporación de grupo al mensaje correspondiente CGMP que es enviado al conmutador, en donde se elimina la asociación del puerto por el cual se emitió el mensaje IGMP original con el grupo.

5. MODELAJE DE ESCENARIO

Elementos y eventos del sistema

Se propone la aplicación de un enfoque por eventos para la conformación del modelo. El estado de cada uno de los elementos, dependerá de un proceso interno individual así como del resultado de la transmisión y recepción de entidades (tramas ethernet). Para ello, es necesario definir los elementos del sistema, y los eventos asociados:

Terminal H.323: constituye un nodo que envía entidades (tramas ethernet) las cuales contienen mensajes de voz y video comprimido (UIT H.323), mensajes de Gestión de Grupos Internet (IGMP) y mensajes de membresía de grupo (IGMP Snooping, GMRP). Se estudiará la versión 2 del protocolo IGMP ya que se definen mensajes Leave Group (No soportados por la versión 1) y presenta gran similitud con la versión 3 [10]. También, es la versión mejor documentada en libros y revistas [13]. Este elemento contiene también un registro de entrada y otro de salida representados como arreglos. En el escenario, se presentan tres elementos terminales:

- 1) Terminal A: transmite video y audio al receptor B constantemente, y al receptor C mientras que este último pertenezca al mismo grupo de los tres terminales.
- 2) Terminal B: recibe video y audio del terminal A constantemente.

- 3) Terminal C: recibe video y audio del terminal A mientras pertenece al grupo de multidifusión.

Las operaciones que realizan son: transmisión y recepción de entidades (tramas ethernet).

Enrutador: constituye un nodo que envía y recibe entidades (tramas ethernet) que contienen mensajes de Gestión de Grupos Internet (IGMPv2) [13] o CGMP. Los primeros pueden ser de Consulta General y de Consulta Específicos, y los segundos pueden ser de adherencia o desincorporación de grupo como resultado del mapeo de mensajes IGMP en mensajes CGMP. Este objeto contiene también un registro de entrada y otro de salida representados como arreglos. En relación a este caso de estudio se puede considerar, que el enrutador posee sólo un puerto, y que las operaciones que se realizan a través del mismo son: transmisión y recepción de entidades (tramas ethernet).

Conmutador ethernet: constituye un nodo que recibe y envía entidades (tramas ethernet) que contienen mensajes de voz y video comprimido (UIT H.323), mensajes de Gestión de Grupos Internet (IGMPv2) [13] o mensajes de membresía de grupos (IGMP Snooping, CGMP y GMRP). Estos protocolos se emplean para llenar y borrar dinámicamente las entradas de la tabla de atributos (Grupos Multicast) CAM. Dicha tabla consiste en una matriz de n filas por m columnas, en donde las filas corresponden a entradas de la tabla asociadas a grupos IP Multicast, y las columnas representan: dirección MAC de grupos IP Multicast, (Ej. 0x0100.5E01.0203) y números de puertos asociados (ver tabla 1).

Tabla 1. Ejemplo de representación de la Tabla CAM

Dirección MAC de Grupo	P1	P2	P3	P4
0x0100.5E01.0203	1	1	0	0

En la Tabla 1 se muestra una entrada, en donde se indican los puertos pertenecientes al grupo IP Multicast 224.1.2.3 (n=1 ; m=5), los puertos 1 y 2 están conectados a anfitriones de grupo directamente o a través de concentradores. Los puertos 3 y 4 no poseen anfitriones de grupo. Este objeto contiene también una matriz de registros de entrada y otra de salida asociados a puertos representados en una matriz. En la tabla 2, se muestra una matriz de ejemplo con 3 filas (Puertos) y 3 columnas (Número de puerto, buffer de entrada y buffer de salida).

Tabla 2. Ejemplo de representación de puertos con registros de entrada y salida

Número del puerto del conmutador	Registros de entrada	Registros de salida
1	ENTRADA	SALIDA
2	ENTRADA	SALIDA
3	ENTRADA	SALIDA
4	ENTRADA	SALIDA

Las operaciones que se realizan con el conmutador son: creación y eliminación de entradas de grupos en tabla CAM (Filas), adición y/o eliminación de números de puertos en cada entrada, transmisión / recepción de entidades (tramas ethernet). En este caso de estudio, se dispone de 4 puertos (uno conectado a cada terminal H.323 y otro conectado al enrutador).

Tipos de tramas

Cada uno de los elementos que conforman al sistema, intercambian información en unidades de datos de protocolos, con un formato distinto dependiendo del tipo de protocolo de membresía de grupo IP Multicast encapsulado en las tramas. Se definen 11 tipos de tramas de mensajes:

1) Tipo 1 (Tráfico de videoconferencia): son enviadas desde el emisor (Terminal A) hacia el grupo de receptores de la sesión de videoconferencia (Terminales B y C). Es importante destacar que se emplean segmentos UDP para la transmisión, y que estas entidades son enviadas con una distribución probabilística en donde los parámetros dependen de las características de dicho tráfico. El tipo y los parámetros de dicha distribución, para realizar el proceso de simulación se determinará en trabajos posteriores, como resultado de la caracterización del tráfico.

2) Tipo 2 (Mensaje IGMPv2 Join): son enviadas desde el terminal C hacia los terminales A y B considerados en el escenario, con la finalidad de manifestar su intención de recibir tráfico dirigido al grupo Multicast.

3) Tipo 3 (Mensaje IGMPv2 Leave): son enviadas desde el terminal C hacia la dirección 224.0.0.2 (Todos los enrutadores conectados a la subred) del escenario, con la finalidad de manifestar la intención de desincorporarse del grupo de sesión.

4) Tipo 4 (Consulta General IGMPv2): son enviadas desde el enrutador hacia la subred conectada al puerto (Conmutador ethernet con terminales A,B y C conectados). Se aplica en el mecanismo de consulta-respuesta del protocolo IGMPv2.

5) Tipo 5 (Consulta Específica IGMPv2): son enviadas desde el enrutador hacia los miembros de un grupo específico, con la finalidad de verificar si un puerto del enrutador está conectado a miembros de activos de dicho grupo.

6) Tipo 6 (Reporte IGMPv2): son enviadas por parte de cualquiera de los terminales que pertenecen al grupo IP Multicast activo, bajo el mecanismo de consulta-respuesta [20].

7) Tipo 7 (Join Empty, GMRP): se usa para declarar un atributo (Pertenencia a un grupo) , en donde el declarante no lo ha registrado de otro. Es enviado por un terminal de videoconferencia.

8) Tipo 8 (Join In, GMRP): se usa para declarar un atributo (Pertenencia a un grupo), en donde el declarante ha hecho el proceso de registro. Es enviado por un conmutador.

9) Tipo 9 (Leave In, GMRP): se usa para eliminar un registro de atributo, para un grupo que todavía tiene miembros. Es enviado por un conmutador al terminal (A) y del terminal (C) al conmutador.

10) Tipo 10 (Join, CGMP): se usa para indicar la asociación de un puerto del conmutador a un grupo.

11) Tipo 11 (Leave, CGMP): se usa para indicar la desasociación de un puerto del conmutador a un grupo.

Modelaje del sistema

Considerando los elementos del sistema, y su interrelación en base al escenario planteado dependiendo del protocolo de membresía de grupo utilizado, se puede caracterizar el comportamiento del sistema con 14 eventos.

1) Transmisión de tráfico de videoconferencia desde el terminal A (Fuente) hasta el terminal B. Envío de tramas tipo 1.

- 2) Transmisión de tráfico de videoconferencia desde el terminal A (Fuente) hasta el terminal C. Envío de tramas tipo 1.
- 3) Solicitud de ingreso del terminal C al grupo. Envío de tramas tipo 2 .
- 4) Solicitud de registro del terminal C al conmutador. Envío de tramas tipo 7.
- 5) Solicitud de registro del conmutador al terminal A. Envío de tramas tipo 8.
- 6) Asociación de grupo IP Multicast a puerto del conmutador.
- 7) Desasociación de grupo IP Multicast con puerto del conmutador.
- 8) Envío de mensaje de consulta general IGMP. Envío de tramas tipo 4.
- 9) Envío de mensaje de reporte IGMP por parte de un terminal . Envío de tramas tipo 6.
- 10) Solicitud de salida de grupo por parte del terminal C. Envío de tramas tipo 3.
- 11) Solicitud de consulta específica del enrutador al grupo . Envío de tramas tipo 5.
- 12) Envío de mensaje tipo 10 de inclusión con CGMP desde el enrutador hasta el conmutador.
- 13) Envío de mensaje tipo 11 de exclusión con CGMP desde el enrutador hasta el conmutador.
- 14) Solicitud de eliminación de registro del terminal C al conmutador. Envío de tramas tipo 9.
- 15) Solicitud de eliminación de registro del conmutador al terminal A. Envío de tramas tipo 9.

En cada uno de estos eventos, se intercambian tramas de alguno de los tipos anteriormente explicados entre dos elementos cuyos campos de datos dependen del protocolo de membresía empleado. Un modelo general, debe permitir adaptarse a cualquier simulador en aspectos relacionados a la definición de las entidades, elementos y eventos.

Se han realizado trabajos previos de modelaje y simulación de redes locales para tráfico unicast con el paquete computacional AWESIM [2], sin considerar la posibilidad de transmisión para tráfico multicast. Esto se debe a las limitaciones del simulador, o a la complejidad de la conformación del modelo. Por otra parte, el paquete computacional NS2 no permite realizar un buen modelaje de los procesos de multidifusión según la documentación [7]. Se propone entonces la representación de las entidades como tipos de datos arreglos, ésto con un lenguaje de programación orientado a objetos. Los elementos del sistema pueden representarse como objetos igualmente (excepto los terminales), y los eventos se pueden modelarse como la ejecución de líneas de código, para lo cual se debe utilizar un sistema operativo con procesamiento multihilo (*Multithreaded*). Los terminales se pueden representar con hilos (*Threads*) , que definen instancias presentes. Adicionalmente se propone la utilización de elementos de sincronización entre procesos, tales como Mutex o Semáforos, presentes en diversos sistemas operativos. De manera que el modelo general está definido por un conjunto de instancias de hilos (Terminales) que transmiten y reciben entidades (Tramas) utilizando una red de objetos (Conmutador y enrutador) que a su vez contienen tablas (atributos, entradas) las cuales son modificadas dinámicamente de acuerdo a los eventos. Las variables de rendimiento a ser consideradas en la simulación, pueden ser definidas de manera simple

considerando el reloj principal del sistema operativo y contadores (grado de utilización, jitter, retardo y tasa de pérdida de tramas).

6. CONCLUSIONES.

- 1) La pila de protocolos IP Multicast define un conjunto de procedimientos que pueden ser modelados con un grado de complejidad variable, dependiendo de los detalles del modelo y del simulador que va a ser empleado. Por ende, se recomienda la utilización de un sistema operativo con soporte de procesamiento multihilos como la base fundamental para el modelaje del tráfico de membresía de grupos y no una herramienta comercial, por las facilidades que provee.
- 2) Para la creación de un modelo genérico representativo del comportamiento del sistema asociado al caso de estudio planteado con cada protocolo de membresía de grupos, se necesita definir claramente los elementos y eventos si se desea realizar un enfoque de modelaje por eventos.
- 3) Las tramas que son transmitidas en el caso de estudio, se pueden modelar como entidades que se leen y escriben en los arreglos (registros). También debe ser soportada la capacidad de generarse con una distribución probabilística preestablecida, por lo que se debe hacer una caracterización del tráfico como paso previo a la simulación.
- 4) La representación de los eventos, se puede modelar con la ejecución del código de los hilos (terminales), la manipulación de los atributos de los elementos (Conmutador y enrutador) así como su interacción con elementos de sincronización entre procesos. Esto involucra la transmisión y la recepción de las entidades entre los hilos y los demás elementos.
- 5) El modelo planteado presenta una tendencia a la utilización de variables de estado, conjuntamente con la posibilidad de utilizar la programación orientada a objetos y sistemas operativos multihilos.

8. LISTA DE ABREVIATURAS

CGMP Protocolo de Gestión de Grupos de CISCO (*CISCO Group Management Protocol*)

GARP Protocolo de registro genérico de atributo (*Generic Attribute Registration Protocol*)

GMRP Protocolo de registro GARP Multicast (*GARP Multicast Registration Protocol*)

GDA Dirección de Grupo Destino (*Group Destination Address*)

IGMP Protocolo de Gestión de grupos Multicast (*Internet Group Management Protocol*)

MCU Unidad de Control Multipunto (Multipoint Control Point).

OSI Interconexión de Sistemas Abiertos (*Open Systems Interconnection*).

USA Dirección de Fuente Unicast
(*Unicast Source Address*)

WAN Red de área amplia (Wide access network).

8. REFERENCIAS

- [1] Duc A. Tran, Kien A. Hua and Mounir Tantaoui, A multi-multicast sharing technique for large-scale video information systems, ICC 2002 - **IEEE International Conference on Communications**, vol. 25, no. 1, April 2002, pp. 2496 – 2502
- [2] Montoya Dan El , Díaz Rafael. Modelaje, simulación y Animación de una Red de Área Local Ethernet de dos Concentradores y tres Estaciones de Trabajo, **Memorias de V Jornadas Científico-Técnicas de ULA**, Marzo-2002, pp 297-300.
- [3] George Carle and Ernst W. Biersack, Survey of error recovery techniques for IP-based audio-visual multicast applications, **IEEE Network**, vol. 11, no. 6, November/December 1997, pp. 24 - 36
- [4] Jonathan S. Turner, A Practical Version of Lee's Multicast Switch Architecture, **IEEE Transactions on Communications**, vol. 41, no. 8, August 1993, pp. 1166 – 1169
- [5] K. Ravindran, A Flexible Network Architecture for Data Multicasting in "Multiservice Networks", **IEEE Journal on Selected Areas in Communications**, vol. 13, no. 8, October 1995, pp. 1426 – 1444
- [6] KUMAR V. **MBONE: Interactive Multimedia on the Internet**. New Riders, USA, 1996.
- [7] **Manual de documentación de simulador NS2**. <http://www.isi.edu/nsnam/ns/ns-documentation.html>, consultada el 27/02/2004
- [8] MORENO C. **Análisis Técnico-Económico de Alternativas de Interconexión entre el Campus UCV con sus núcleos para el Servicio de Videoconferencia**. Trabajo especial de Especialización de Redes de Datos, Escuela de Ingeniería Eléctrica UCV, Venezuela, 2001.
- [9] SEIFERT R. **The Complete Guide to LAN Switching Technology**. WILEY, USA, 2001.
- [10] **RFC 3376: IGMPv3**. <ftp://ftp.rfc-editor.org/in-notes/rfc3376.txt>, consultada el 27/02/2004.
- [11] **RFC 2236: IGMPv2**. <ftp://ftp.rfc-editor.org/in-notes/rfc2236.txt>, consultada el 27/02/2004.
- [12] **RFC 1112: IGMPv1**. <ftp://ftp.rfc-editor.org/in-notes/rfc1112.txt>, consultada el 27/02/2004.
- [13] WILLIAMSON B. **Developing IP Multicast Networks**. **Ciscopress**, USA, 2000.